EUROSMART
The Voice of the Digital Security Industry

Cybersecurity Industry Recommendations on the CRA Guidance

Strengthening legal certainty and ensuring consistent implementation of Regulation (EU) 2024/2847

Executive Summary

Industry welcomes the Commission's work on the Guidance on the application of the Cyber Resilience Act (CRA). The Guidance is essential to support manufacturers, importers, distributors, conformity assessment bodies and market surveillance authorities in the practical implementation of Regulation (EU) 2024/2847.

The CRA Guidance is formally non-binding. In practice, however, it will become the principal reference used by economic operators and authorities to interpret the Regulation. Its wording will therefore influence conformity assessment, enforcement expectations, contractual requirements and procurement practices across the Union. For that reason, the Guidance must remain closely aligned with the legislative text and must avoid creating de facto obligations that were not adopted by the co-legislators.

This document aims at improving legal certainty, preserving the CRA risk-based and technology-neutral approach, and ensuring that the Guidance remains practically workable for all Products with Digital Elements (PwDE), particularly software products, open-source ecosystems, complex supply chains and legacy technologies. A key element of this workability is the recognition of existing security evidence from established industry schemes such as CC, ISO 21434, EMVCo, FIPS, SESIP, PSA Certified. This would help mitigate assessment bottlenecks and safeguard market resilience during the CRA transition.

This position paper restructures the outstanding recommendations around five policy themes:

- **Software products and software systems**
- **Free and Open-Source Software and Open-Source Software Stewards**
- **Substantial modifications**
- **A proportionate approach for complex and legacy environments**
- **Legal certainty and consistent interpretation**

Overview of relevant recommendations by topic

The detailed comments are referenced in each section and included in the Annex I.

Theme	Relevant comments	Purpose of the recommendations
Software products and software systems	Comments 1, 2 and 3	Clarify software systems, software formats, integrated software modules, user of software product and vulnerability handling for subsequent substantially modified versions of a software product.
FOSS and Open-Source Software Stewards	Comments 4, 5 and 6	Clarify intended commercial activities, steward status, public visibility and not-for-profit treatment.
Substantial modifications	Comments 7 and 8	Clarify that internal design changes, configuration and loading of data are not substantial modifications where they do not affect compliance or intended purpose.
Legacy products and conformity assessment	Comments 9, 10, 11 and 12	Clarify combined conformity assessments, legacy interoperability, risk treatment and proportionate review.
Legal certainty and interpretation	Comments 13 to 21	Clarify core functionality, RDPS, external dependencies, reporting obligations and B2B tailor-made/subcontracting, consortium scenarios.

The CRA Guidance must remain a practical interpretation of the CRA

The CRA introduces a horizontal cybersecurity framework for PwDE. Its successful implementation depends on the ability of manufacturers and other economic operators to understand their obligations, assess cybersecurity risks and demonstrate conformity in a proportionate and predictable manner.

The Commission Guidance should therefore perform three functions. First, it should clarify the meaning of key legal concepts without modifying them. Second, it should provide examples that help economic operators apply the CRA in concrete cases. Third, it should support a harmonised interpretation by market surveillance authorities and notified bodies across the Union.

The recommendations identified in this paper should be understood in that context. **They are not requests for exemptions.** They are requests for precision. They aim to prevent uncertainty in areas where the draft Guidance could otherwise be interpreted differently by manufacturers, notified bodies, customers and national authorities.

1. Software products and software systems

The CRA applies to software and hardware products with digital elements. However, modern software products do not always fit neatly into traditional product concepts developed for hardware. Software may be supplied as source code, compiled binaries, container images, install files, download links or other digital artefacts. It may also be supplied as a set of modules that are intended to be installed and operated together as a single software system. In addition, the very nature of software, which can be accessed remotely, raises a particular question regarding the identification of that software product's users. The case of vulnerability handling of an earlier version of a software product, where that earlier version is not present in the field anymore, should also be clarified.

A product-level approach for modular software

The outstanding recommendations seek to ensure that the Guidance clearly distinguishes between individual software components and the software product or software system that is placed on the market. This distinction is essential because a manufacturer may supply several software elements – such as SDKs, libraries, installers, container images, reference modules or configuration packages – which are not marketed separately but are intended to form one product with digital elements once installed and integrated according to the manufacturer's instructions. [Comments 1, 2 and 3].

Software systems composed of multiple components

In the same way as there is a sub-section discussing "complex systems" (§2.5), a dedicated sub-section should be added within section 2 to deal with "software systems" comprising several software components, but no hardware. Such a clarification is needed where several distinct software components are supplied separately, but only together constitute the product placed on the market. In these scenarios, the Guidance should clarify that individual software components developed by the supplier should not automatically be considered separately placed on the market where they are never supplied independently as stand-alone products.

Instead, the CRA obligations should be attached to the software system as the product placed on the market, while the individual components are considered within that product's cybersecurity risk assessment and technical documentation.

This clarification is particularly important where a software system contains a combination of components developed by the supplier, third party proprietary components distributed by the supplier, and Free and Open-Source Software components. The Guidance should explain whether such components are to be treated as integrated components subject to due diligence under Article 13(5), as external dependencies, or under another category. Without this clarification, similar software supply models could be interpreted differently across Member States. **[Comment 1].**

Different software formats, one legal product

This point should be complemented by requesting clarification that a software product may be supplied in different technical forms without changing its legal nature. Source code, compiled files and containers may represent the same software product. The form in which software is supplied should not, by itself, determine the cybersecurity risk assessment or the applicability of essential cybersecurity requirements. Once conformity has been demonstrated for the software product, the Guidance should clarify that the product may be placed on the market in any of these forms, provided that the relevant cybersecurity characteristics remain covered by the assessment. **[Comment 2].**

Integrated software modules

The CRA Guidance should include an example illustrating software modules supplied solely as part of an integrated product and not made available separately. Such an example would be valuable for manufacturers supplying a set of software elements – for instance SDKs and libraries – that collectively form a data management product. The individual elements should not be treated as separately placed on the market where they are exclusively supplied as part of the integrated product. **[Comment 3].**

The CRA Guidance should reflect contemporary software development and deployment models. Doing so would strengthen legal certainty without reducing cybersecurity assurance, since the software system as a whole would remain subject to the CRA requirements, including cybersecurity risk assessment, conformity assessment, vulnerability handling and reporting obligations.

User of software product

It should also be better clarified who the user – as per the CRA – is for software products. Some software products are intended to be installed and operated on a server, and accessed remotely by a third party, without any component installed on the third party's side or device (zero footprint). In such settings, the third party accesses a remote service but is not supplied with the software product for distribution or use.

Therefore, the CRA guidance should clarify that in such case, the third party is not a user of the software product.

Vulnerability handling for software versions no longer in use

Another topic relates to Article 13(10) regarding vulnerability handling on an earlier version of software products. In some cases, a manufacturer can ensure that an earlier version of a software product is not present anymore in the field, as its customers have all migrated to the latest version of the software product. For instance, this is the case in the context of a B2B transaction, for which software products for professional use are placed on the market. In such cases, the manufacturer has exhaustive and complete knowledge of who is using its software products as well as their version.

Therefore, where the manufacturer can demonstrate that an earlier version of a software product is not present anymore in the field, the CRA guidance should clarify that the manufacturer is not required to ensure compliance of that earlier version of the software product with any essential requirements of Annex I, Part 2.

2. Free and Open-Source Software and Open-Source Software Stewards

The CRA contains a carefully balanced approach to Free and Open-Source Software (FOSS). It recognises the specific nature of open-source development while introducing targeted obligations for Open-Source Software Stewards. The Guidance should preserve this balance and avoid interpretations that create uncertainty for foundations, not-for-profit entities, maintainers, contributors and manufacturers integrating FOSS into their own products.

The outstanding recommendations focus on three issues: the meaning of FOSS intended for commercial activities, the ability of third parties to identify whether an entity is a steward, and the treatment of not-for-profit organisations in the FOSS decision flow. **[Comments 4, 5 and 6].**

Determining whether FOSS is intended for commercial activities

A fundamental question arises regarding the criterion that a FOSS product be "ultimately intended for commercial activities". The Guidance should clarify whose intention is relevant and how that intention is to be established. Is the relevant intention that of the entity maintaining or publishing the FOSS? Is it sufficient for the entity to publicly state that the software is intended for commercial integration? Or can the criterion be met simply because the FOSS is used commercially by third parties, potentially without the knowledge of the publishing entity?

This distinction is critical. If steward status depends on the intention and conduct of the publishing entity, legal obligations are predictable and can be managed. If steward status can arise merely because third parties use the FOSS in commercial products, an entity could become subject to obligations without knowing that the relevant criterion has been met. The Guidance should therefore provide objective indicators for determining whether FOSS is intended for commercial activities. **[Comment 4].**

Making steward status identifiable to third parties

The current situation leads to damaging consequences: manufacturers integrating FOSS need to know whether they are relying on software supported by a steward, particularly for due diligence and vulnerability handling. The draft Guidance appears to recommend that entities which no longer provide sustained support should inform others, but it is unclear whether there is an

obligation to do so. The recommendation requests a public and accurate list of stewards, as well as clear communication when an entity stops providing sustained support for a FOSS project. If such a list cannot be established directly through the CRA Guidance, the Commission should provide clarification on how manufacturers can reasonably identify steward status and how they should treat cases of uncertainty**. [Comment 5].**

Avoiding automatic classification of not-for-profit entities

Other concerning question is the flowchart for FOSS coverage. The direct link between the box "Are you a not-for-profit organisation?" and "Open-Source Software Steward" is ambiguous. Recital 18 and the draft Guidance itself suggest that not all not-for-profit organisations are necessarily stewards. A not-for-profit organisation may publish FOSS without meeting all elements of the steward definition. The flowchart should therefore avoid suggesting that not-for-profit status automatically leads to steward status. The more accurate decision path would require a further assessment of whether the FOSS is intended for commercial activities and whether the entity systematically provides sustained support and ensures viability.

The Commission should ensure that the Guidance provides objective, transparent and operational criteria for FOSS and steward status. This would support the European open-source ecosystem while preserving the CRA's policy objective of improving cybersecurity where open-source software is systematically supported for commercial use. **[Comment 6].**

3. Substantial modifications

The concept of substantial modifications is central to the CRA lifecycle framework. It determines when changes to a product trigger regulatory consequence, including potentially new conformity assessment procedures and a new placing on the market. For that reason, the CRA Guidance should provide criteria that are objective, predictable and proportionate.

The outstanding recommendations seek to clarify that not every change to a product with digital elements should be treated as a substantial modification. This is particularly important for software-intensive products, where internal architecture, dependencies, modules, libraries and configuration parameters may evolve throughout the product lifecycle. **[Comments 7 and 8].**

Internal design changes and normal engineering evolution

Changes to the internal design of a product should not be considered substantial modifications where two cumulative conditions are met: the change does not affect compliance with the essential cybersecurity requirements, and it does not modify the intended purpose for which the product was originally assessed. Examples include the use of new COTS[1], use of new internal services or features from COTS or software module, replacement of one software module by another. These changes may be part of normal engineering evolution and maintenance. They should not automatically trigger a new regulatory classification if the product's cybersecurity characteristics and intended purpose remain unchanged. **[Comment 7].**

[1] Commercial Off the Shelf" (https://en.wikipedia.org/wiki/Commercial_off-the-shelf).

Configuration and data loading under manufacturer instructions

The CRA Guidance should explicitly state that configuring a product with digital elements or loading data into such a product in accordance with the manufacturer's information, instructions or guidance, is not a substantial modification. This point is especially important for professional and industrial users, where products are often configured for a specific operational environment. Treating ordinary configuration as a substantial modification would create significant legal uncertainty and could discourage users from following manufacturer instructions.

The Commission should therefore reconsider the CRA Guidance to make clear that the decisive criteria are the effect of the change on the product's intended purpose and on compliance with the essential cybersecurity requirements. This would preserve CRA's risk-based approach and avoid creating unnecessary barriers to maintenance, configuration, optimisation and lifecycle management. **[Comment 8].**

4. A proportionate approach for complex and legacy environments

The CRA applies across highly diverse sectors, including ones where long product lifecycles, interoperability constraints and legacy standards are unavoidable. The Guidance should therefore support a proportionate transition to CRA compliance and provide sufficient clarity on conformity assessment in complex or legacy environments.

The outstanding recommendations address conformity assessment, legacy interoperability, risk treatment and the proportionality of review activities. **[Comments 9, 10, 11, and 12].**

Recognition of existing assurance evidence (CC, ISO 21434, EMVCo, FIPS, SESIP, PSA)

The CRA's applicability to legacy products (designed and produced before the 11th of December 2027 but placed on the market thereafter) creates acute compliance and continuity risks. Key implementation elements remain unsettled, including harmonised standards, delegated acts, interpretative guidance, certification procedures, and market surveillance practices. At the same time, non-compliance can lead to significant sanctions or loss of market access.

A full, subsequent conformity assessment of legacy products will be resource-intensive and, for important class I, class II and critical products, will likely face bottlenecks at external conformity assessment bodies. The resulting delays and costs risk product discontinuations, particularly among mature products and semiconductor components, diverting funds and capacity from research and innovation and threatening supply continuity.

To mitigate these risks without compromising security outcomes, the Guidance should:

- recognise existing security evidence from credible national or industry schemes (e.g., Common Criteria national schemes, ISO 21434, EMVCo, FIPS, SESIP, PSA Certified) as valid inputs toward CRA requirements;
- accept targeted manufacturer declarations to cover narrowly scoped gaps where existing evidence does not map fully to CRA obligations, supported by technical justifications and risk analyses;

- encourage notified bodies to adopt and foster this recognition approach, including agreed equivalence mappings, streamlined reviews for legacy products, and an emphasis on proportionality and non-duplication.

This pragmatic path preserves security assurance, reduces assessment bottlenecks, avoids unnecessary rework, and protects Europe's innovation capacity and market resilience during the CRA transition.

Combining conformity assessment routes

Combining several conformity assessment approaches is not sufficiently addressed. Manufacturers may need or wish to combine different assessment routes, for example Module B+C and Module H for vulnerability handling requirements, or certificates such as EUCC where they create a presumption of conformity for certain requirements. The Guidance should explain how multiple conformity assessments may be combined to demonstrate conformity with the essential cybersecurity requirements and, where relevant, to benefit from a presumption of conformity.

In addition, this clarification should address practical questions.

- Must the assessments be based on the same cybersecurity risk assessment?
- Must they relate to exactly the same product configuration?
- Must they collectively cover all essential requirements, or all identified risks?
- Can one essential requirement or one cybersecurity risk be covered through a combination of assessments, or must it be covered entirely by a single assessment route?

The Guidance should also recognise that in such scenario conformity may be assessed by more than one conformity assessment body. Without clear rules, manufacturers and notified bodies may adopt inconsistent approaches. **[Comment 9].**

Legacy interoperability as part of the intended purpose

Some products must support legacy algorithms, mechanisms or protocols for interoperability reasons. This is not a marginal issue. For some verticals such as electronic travel documents, payment cards, health, banking or other international ecosystems, products often need to interoperate with infrastructures that evolve slowly and involve many stakeholders. The CRA Guidance should clarify how manufacturers should address cybersecurity risks where the use of legacy mechanisms is part of the intended purpose and market reality of the product.

In such cases, the CRA Guidance should avoid implying that products can no longer be placed on the market merely because they support mechanisms that are not state of the art. Likewise, the Guidance should clarify that the manufacturer is not liable for the presence of legacy algorithms, mechanisms or protocols which stem from their intended purpose. Instead, it should explain how such risks should be documented in the cybersecurity risk assessment, how residual risks may be handled, and whether mitigation may include measures outside the product itself. The Guidance should also consider whether concepts currently discussed in relation to complex systems should be relocated or broadened so that they also apply to legacy interoperability requirements outside complex systems. **[Comment 10].**

Risk treatment beyond embedded product measures

Moreover, risks should not always have to be addressed through product-level measures. In some cases, manufacturers may mitigate risks by providing information and instructions to users, for example where secure use depends on deployment conditions, interoperability constraints or operational procedures. The Guidance should recognise that risk mitigation may include product-level measures, user instructions and other appropriate measures depending on the nature of the risk and the product's intended purpose. **[Comment 11].**

Organisational, physical and technological security controls

Security controls may be organisational, physical or technological. This is important because cybersecurity is not always achieved exclusively through technical measures embedded in the product. Contractual arrangements, operational procedures, physical protection, service level commitments and organisational controls may be relevant to the treatment of certain risks, especially where the product relies on external services or is deployed in professional environments. This approach should be clarified in the document. **[Comment 12].**

5. Legal certainty and consistent interpretation

The remaining outstanding recommendations are cross-cutting. They concern legal certainty in areas where uncertainty could have significant operational consequences for manufacturers, integrators, service providers and authorities. These include core functionality, remote data processing solutions, external dependencies, reporting obligations and B2B manufacturing arrangements.

Core functionality

The CRA Guidance should clarify that a product shall always have a single core functionality for the purpose of determining the applicable conformity assessment regime. [Comment 13].

Remote data processing solutions, components and external dependencies

On remote data processing solutions (RDPS) and the distinction between components, RDPS and external dependencies, the CRA Guidance should clearly distinguish between cases where the software for remote data processing is designed and developed by the manufacturer or is under its responsibility, and cases where a manufacturer merely relies on a third-party solution not designed or developed under its responsibility. Where the answer to the relevant RDPS criterion is negative, the Guidance should not automatically treat the third-party solution as a component of the product. It may be more appropriate to treat it as an external dependency, with different consequences for risk assessment and due diligence. [Comments 14, 15 and 16].

Where both relevant RDPS conditions are met, the data processing solution should be treated consistently in the risk assessment and, where appropriate, subject to due diligence. Where a third-party solution does not qualify as RDPS because it was not designed or developed by the manufacturer or is under its responsibility, it should be treated as an external dependency rather than as a component. The corresponding figure should be clarified, as its current logic may suggest that non-RDPS third party data processing is nevertheless treated as a component. This

distinction is essential for manufacturers seeking to correctly scope their CRA obligations. **[Comments 14 and 15].**

Reporting obligations: criteria, overlap and temporal scope

Criteria should be established for determining when a vulnerability is "actively exploited". This is essential because reporting obligations depend on this qualification, and manufacturers need operational criteria that can be applied consistently by product security teams. [Comment 17]. Further clarification of the temporal limit of reporting obligations should be including and specifying that they should apply until the support period of the last product placed on the market has expired. Without such clarification, manufacturers may face uncertainty about potentially indefinite obligations for products no longer supported, no longer placed on the market or no longer used in the field. **[Comment 18].**

Regarding the relationship between "actively exploited vulnerabilities" and "severe incidents having an impact on the security of the product with digital elements", the CRA Guidance should clarify whether these are intended to be mutually exclusive categories or whether a single event may fall under both. If overlap is possible, the reporting process should be streamlined to avoid duplicate or inconsistent submissions. If the categories are intended to be distinct, the Guidance should provide criteria for delineating them. This is important not only for compliance, but also for the efficient operation of the single reporting platform. **[Comment 19].**

For the temporal scope of reporting obligations as from September 2026, the Guidance should clarify whether the reporting obligations apply to any product with digital elements placed on the market from that date onwards, or whether they also apply to products placed on the market before that date. This is a major implementation issue. Applying reporting obligations retroactively to products already placed on the market would create a significant and immediate operational burden, while a prospective interpretation would allow manufacturers to ramp up compliance obligations alongside the placing on the market of new products. **[Comment 20].**

B2B tailor-made products and subcontracting

The CRA Guidance should clarify the particular case of B2B tailor-made products that are designed, developed or manufactured according to customer specifications.

In this context, the CRA Guidance should clarify the distinction between placing a tailor-made product on the market and acting as a subcontractor for a customer who is the manufacturer. This question is critical for companies operating in B2B contexts, where products may be developed specifically for one customer or according to customer requirements. The Guidance should identify the key criteria for determining who is the manufacturer, who places the product on the market, and when a transaction is better characterised as subcontracted design, development or manufacturing. **[Comment 21].**

In addition, it should be explicitly clarified that the CRA does not prevent nor affect the possibility for stakeholders to team up into a consortium to make products with digital elements available on the market. In such cases, the provisions set forth by the CRA for the manufacturer, importer, distributor and the product with digital elements apply in the same way, and the nature of the economic operator, i.e. consortium, legal person, has no impact.

Conclusions & recommendations

In light of the above, some key recommendations for the Cybersecurity Industry must be reconsidered or at least clarified. In particular:

- clarification on software systems composed of multiple software components supplied to operate together as one product with digital elements;
- clarify that the technical form in which software is supplied – source code, compiled file, container or other equivalent form – does not by itself determine its legal treatment or risk assessment;
- clarify that a third party using a software product remotely (software installed on a server providing a service) is not a user of that software product;
- clarify that where the manufacturer can demonstrate that an earlier version of a software product is not present anymore in the field, the manufacturer is not required to ensure compliance of that earlier version of the software product with any essential requirements of Annex I, Part 2;
- provide objective criteria for identifying FOSS intended for commercial activities and for determining Open-Source Software Steward status, while avoiding the suggestion that not-for-profit status automatically leads to steward status;
- clarify how third parties can identify whether an entity is a steward and how manufacturers should treat uncertainty in their due diligence and vulnerability handling processes;
- state expressly that internal design changes, configuration and loading of data are not substantial modifications where they do not affect compliance with the essential cybersecurity requirements or the intended purpose of the product;
- clarify how conformity assessment approaches may be combined and how multiple assessments may collectively demonstrate conformity;
- recognise existing security evidence from credible national or industry schemes (e.g., Common Criteria, ISO 21434, EMVCo, FIPS, SESIP, PSA Certified) as valid inputs toward CRA requirements to protect market resilience during the CRA transition;
- recognise that legacy interoperability requirements may be part of a product's intended purpose and should be addressed through the cybersecurity risk assessment rather than treated as an automatic barrier to market access, and that in such case the manufacturer shall not bear any supplemental liability;
- recognise that risk mitigation may include product-level measures, user instructions, organisational measures, contractual arrangements, physical protections and other appropriate controls;
- clarify that there shall be a single core functionality;
- clarify the distinction between RDPS, components and external dependencies, especially where third party data processing solutions are not designed or developed by the manufacturer or under its responsibility;
- provide operational criteria and temporal boundaries for reporting obligations, including actively exploited vulnerabilities, severe incidents and products placed on the market before or after the reporting date;

- clarify B2B tailor-made product and subcontracting scenarios so that the identity of the manufacturer and the allocation of CRA obligations can be determined predictably, while explicitly confirming that the CRA does not prevent stakeholders from teaming up into a consortium to make products with digital elements available on the market.

An improved guidance that reflects these elements would better support manufacturers, notified bodies and market surveillance authorities, while contributing to the common objective of a high and consistent level of cybersecurity across the European Union.

Annex I : Full Comments on CRA Guidance

No.	Org.	Item	Comments	Proposed change
1	ES	S.2	In the same way as there is a section discussing "complex systems" (§2.5), a dedicated section should be added within section 2 to deal with "software systems" comprising several software components, but no hardware. A software system comprises several distinct software components (e.g. SDK, libraries…), and each software components is supplied as a stand-alone component (e.g. under the shape of separate files, install files, download links or URL). All these software components once installed and integrated all together as documented by the supplier comprises a product with digital element ("software system"). Some of these software components may be designed, developed and manufactured by the supplier (therefore being their manufacturer), some others may be distributed by the supplier (therefore being their distributor), and some other may be FOSS. This situation is very common in many sectors. This new section should clarify the following aspects: • Each individual software components designed, developed and manufactured by the supplier shall not be considered placed on the market nor subject to the CRA, provided they are never placed on the market separately. In such case, only the "software system" shall be considered placed on the market and subject to the CRA; • Where the supplier has designed, developed and manufactured one or several of the software components, how should be treated the other software components (those for which the supplier is distributor and the FOSS)? Should they be treated as third party components integrated in its "software system" and thus covered by the	Add a dedicated section on that topic in section 2 and clarify these aspects.

			due diligence (article 13.5)? Should they be treated as external dependencies of the environment of the "software system"? other? • Where the supplier does NOT design, develop and manufacture ANY of the software components but only distribute software components (distributor of PwDE manufactured by others) and possibly supply FOSS, together with its own documentation to install and integrate them, what is the role of the supplier as per the CRA? Manufacturer of the "software system"? Distributor of the PwDE manufactured by others? Other? If it is a "manufacturer", how should be treated the software components? Should they be treated as third party components integrated in its "software system" and thus covered by the due diligence (article 13.5)? Should they be treated as external dependencies of the environment of the "software system"? other?	
2	ES	S.2	Clarifications should be brought regarding software in a new paragraph 1. It should be clarified that a software may be supplied under various shape: source code, compiled file (install file or file which may be either sent by mail, downloaded or given on a physical medium such as an USK key) or container (to be executed on a Container runtime systems) containing the software; 2. It should be clarified that these three shapes are three representations of the same software product with digital elements; It should be clarified that the shape of the software product is not relevant for the cybersecurity risk assessment and the implementation of the essential cybersecurity requirements;	Add a dedicated paragraph and section.

			3. It should be clarified that after successful conformity assessment, a software product with digital element may be placed on the market in any of these three shapes;	
3	ES	P.145	An example should be added to illustrate the following statement "This is without prejudice to modules supplied solely as components of an integrated product with digital elements and not made available separately; in such cases, the core functionality is determined at the level of the integrated product with digital elements" See proposal.	Add the following new example: "A manufacturer supplies several distinct software's (e.g. SDK, libraries,..) under the shape of e.g. separate files, install files, download links or URL to a customer, which altogether, once installed and integrated as documented by the manufacturer comprises a product with digital element for data management. The SDK and some of these libraries supplied by the manufacturer are never placed on the market separately as they are exclusively supplied as part of the placement on the market of that product with digital element for data management. Therefore, the individual SDK and libraries are not placed on the market and are not subject to the CRA. Only the product with digital element for data management comprising the individual SDK and libraries is placed on the market and subject to the CRA obligations (e.g. definition of intended purpose, cybersecurity risk assessment, conformity assessment, reporting obligations,...) - which indirectly indeed covers the individual SDK and libraries."
4	ES	P.71	It should be clarified how the criteria whereby a FOSS is 'ultimately intended for commercial activities, such as for integration into commercial services or into monetised products with digital elements' (recital 19 of the CRA) shall be established. 1. Should these criteria be established where the entity states so publicly (e.g. on its website, rulebook...)? => In such case being a "steward" is a decision of the entity itself 2. Should these criteria be established where the FOSS happens to be used for commercial activities, possibly without the entity knowing it? => In such case being a	To be clarified

			"steward" is not a decision of the entity itself, and may not even be known by the entity itself More globally, the following points SHALL be clarified: • Intended by whom? The entity maintaining the FOSS? The ones integrating that FOSS? • How does this intention materialise?	
5	ES	P.83	It is still unclear how a third party can guess whether an entity is a steward for a FOSS or not. This paragraph recommends entity which do not provide any more sustained support to inform that they are not steward anymore. Therefore, it means they are not required to do so. However, it has substantial consequences for third party relying on that steward's FOSS and more precisely its vulnerability handling. Therefore, it is critical that this information is accurate, and communicated in due time to everyone, in particular as it will be duly considered in the due diligence of and vulnerability handling provided by manufacturers integrating that FOSS. Therefore: 1. a public and accurate list of stewards shall be put in place and maintained to support manufacturers 2. there shall be obligation for steward to communicate publicly and within a short time frame when they stop to provide sustained support for some of their FOSS.	1. a public and accurate list of stewards shall be put in place and maintained to support manufacturers 2. there shall be obligation for steward to communicate publicly and within a short time frame when they stop to provide sustained support for some of their FOSS.
6	ES	F.1	On which part of the CRA does the link between the boxes "Are you a not-for-profit organisation?" and "Open-Source software steward" rely? As per recital (18), not-for-profit organisation may not necessarily be an Open-Source Software steward. This interpretation is confirmed by P.66 which confirms that "not-for-	Clarify the rationale of that link. It rather seems that the arrow "Yes" leaving the box "Are you a not-for-profit organisation?" should go to the box "Is the FOSS intended for commercial activities?"

			profit organisation" may not be "Open-Source Software steward" Therefore, it rather seems that the arrow "Yes" leaving the box "Are you a not-for-profit organisation?" should go to the box "Is the FOSS intended for commercial activities?"	
7	ES	P.111	It should be explicitly stated that modification whereby the internal design of the product with digital element is changed (e.g. use of new COTS, use of new internal services or features from COTS or software module, replacement of one software module by another one,...) while not (1) affecting the product's compliance with the essential cybersecurity requirements and (2) modifying the intended purpose for which the product was originally assessed (see P.99) is not a substantial modification. Note : COTS = "Commercial Off The Shelf" (https://en.wikipedia.org/wiki/Commercial_off-the-shelf)	Add the following text: "Modification whereby the internal design of the product with digital element is changed (e.g. use of new COTS, use of new internal services or features from COTS or software module, replacement of one software module by another one...) while not (1) affecting the product's compliance with the essential cybersecurity requirements and (2) modifying the intended purpose for which the product was originally assessed (see P.104) is not a substantial modification."
8	ES	S.4.4.1	It should be explicitly clarified that the configuration of a product with digital elements, or the loading of data within a product with digital elements in accordance with the information and instructions to users or guidance provided by the manufacturer is not a substantial modification.	Add the following paragraph: "The configuration of a product with digital elements, or the loading of data within a product with digital elements in accordance with the information and instructions to users or guidance provided by the manufacturer is not a substantial modification."
9	ES	S.6.3	Some manufacturers may wish to combine several conformity assessments approach to fulfil their obligations, i.e. Module B+C and Module H (e.g. for vulnerability handling cybersecurity requirements) or an EUCC certificate (if it brings presumption of conformity) combined with a module H to cover other essential cybersecurity requirements. In such cases:	Clarify the rules for combining several conformity assessments, and in particular 1. what are the rules to "combine" the various conformity assessments all together to demonstrate fulfilment of the essential cybersecurity requirements? 2. what are the rules to "combine" the various conformity assessments all together to benefit from the presumption of

			1. what are the rules to "combine" the various conformity assessments all together to demonstrate fulfilment of the essential cybersecurity requirements? 2. what are the rules to "combine" the various conformity assessments all together to benefit from the presumption of conformity? For instance: 2.1. should it be demonstrated that the various conformity assessments are based on the same cybersecurity risk assessment? 2.2. should it be demonstrated that the various conformity assessments relate to the same product? 2.3. Should it be demonstrated that the various conformity assessments altogether cover all the essential requirements? or cover all the risks? 2.4. Is it possible to have one essential cybersecurity requirement covered by the combination of the various conformity assessments? Or should it be entirely covered by a single conformity assessment? 2.5. Is it possible to have one risk covered by the combination of the various conformity assessments? Or should it be entirely covered by a single conformity assessment? In addition, in such cases, it is highly likely that the conformity of PwDE will be assessed by several CABs and not only one. This should be clearly highlighted	conformity? For instance: 2.1. Should it be demonstrated that the various conformity assessments are based on the same cybersecurity risk assessment? 2.2. Should it be demonstrated that the various conformity assessments relate to the same product? 2.3. Should it be demonstrated that the various conformity assessments altogether cover all the essential requirements? or cover all the risks? 2.4. Is it possible to have one essential cybersecurity requirement covered by the combination of the various conformity assessments? Or should it be entirely covered by a single conformity assessment? 2.5. Is it possible to have one risk covered by the combination of the various conformity assessments? Or should it be entirely covered by a single conformity assessment? In addition, in such cases, it is highly likely that the conformity of product will be assessed by several CABs and not only one. These specificities should be clearly highlighted.
10	ES	S.7	Some products are required by the market for interoperability reasons to support legacy algorithms, mechanisms or protocols which may not be considered at the state of the art. This is the case in many products which are intended to be used in international ecosystems (1) for which - as a result - interoperability is key, but also (2) whose inertia is important (any upgrade involves numerous decisions making entities, very important budget and takes a lot of	Clarify how to address the risk assessment of products which are required by the market for interoperability reasons to support legacy algorithms, mechanisms or protocols which may not be considered at the state of the art.

			time). This is the case for instance for electronic travel document or banking card but also in the health sector and payment sector.... 1. Does it mean that it would not be possible to place such product on the market anymore? 2. In such case how should be treated in the risk assessment the use of these legacy algorithms, mechanisms or protocols, considering that it is usually impossible for manufacturers to mitigate risks by altering the way the product is used as it would impede interoperability (meaning that no technical measures can be implemented in the product to mitigate the risks)? 3. Should the manufacturer bear any responsibilities for vulnerabilities stemming from the use of these legacy algorithms, mechanisms or protocols, considering that their use is a key characteristic of the market and thus of the product and its intended purpose? In addition it seems that paragraph 32, currently located in the section "2.5 Complex systems" is also perfectly applicable to that situation. Therefore, this text should be located in a more generic section - at least not bound to complex systems.	1. Does it mean that it would not be possible to place such product on the market anymore? 2. In such case how should be treated in the risk assessment the use of these legacy algorithms, mechanisms or protocols, considering that it is usually impossible for manufacturers to mitigate risks by altering the way the product is used as it would impede interoperability (meaning that no technical measures can be implemented in the product to mitigate the risks)? 3. Should the manufacturer bear any responsibilities for vulnerabilities stemming from the use of these legacy algorithms, mechanisms or protocols, considering that their use is a key characteristic of the market and thus of the product and its intended purpose? In addition it seems that paragraph 32, currently located in the section "2.5 Complex systems" is also perfectly applicable to that situation. Therefore, this text should be located in a more generic section - at least not bound to complex systems.
11	ES	P.169	"Nonetheless, the CRA requires the manufacturer to address the risk they may pose through product-level measures, [...]" These risks could also be addressed by providing guidance to the users through the information and instruction to user. Therefore, 1. the statement "through product level measures" should be deleted; 2. it should be clarified that these risks may also be addressed by providing guidance to the users through the information and instruction to user.	1. delete the statement "through product level measures"; 2. Add the following text before the end of the sentence: "[...] or by providing guidance to the users through the information and instruction to user."

12	ES	P.208	It should be clarified that the security controls may be of various kinds: organizational controls (including contractual agreement with third party), physical controls and technological controls.	Clarify that the security controls may be of various types : organizational controls (including contractual agreement with third party), physical controls and technological controls.
13	ES	P.144	A product with digital elements may not have more than one core functionality for the purposes of determining the applicable conformity assessment regime." This wording is unclear. It should be clear whether the product shall be considered to have a single core functionality or whether it may have several.	Make very clear whether the product shall be considered to have a single core functionality or whether it may have several.
14	ES	P.202	Note: A major misunderstanding here. If this comment is not accepted, further clarifications are definitely needed to help understanding the reasoning behind. **Item c** The text seems incorrect. If the answer to the question in "8.1.3 Has the software been designed and developed by the manufacturer, or under its responsibility?" is negative, the data processing does not qualify as RDPS and thus is not part of the PwDE and thus shall not be treated as a "component" as stated in the first line, but rather as "external dependencies". In addition, in such case 1. there is no obligation of due diligence for the manufacturer, and 2. the wording "integration of" should be replaced by "dependency on" More generally this statement comes without explanation or rationale in the previous paragraph justifying this conclusion. If this statement is true, it should be further explained in dedicated paragraph.	1. Change the text as follows: "Manufacturers should treat the third party solution as an external dependency if the answer [...]" 2. Remove the following text :"Additionally, manufacturers should exercise due diligence." 3. Change the sentence as follows : "[...] from the dependency on such solution and mitigate them accordingly [...]"

15	ES	P.202	Note: A major misunderstanding here. If this comment is not accepted, further clarifications are definitely needed to help understanding the reasoning behind. **Item b** It should be clarified that in such case, the data processing shall be treated as an “external dependency”	Add the following text: "The third-party solution shall be treated as an external dependency."
16	ES	F.9	Note: A major misunderstanding here. If this comment is not accepted, further clarifications are definitely needed to help understanding the reasoning behind. This figure is very unclear. 1. For which reason when the answer to "Is such remote data processing developed under your responsibility?" is no, the data processing should be treated as a "component"? As it does not qualify as RDPS, it is not part of the PwDE. Therefore, it should be treated as an "external dependencies" 2. In the box 'CRA RDPS", it should be further clarified that the third party resources (e.g. IaaS, PaaS,...) required for the execution of the software for remote data processing designed and developed by the manufacturer, or under its responsibility SHALL be treated as a "component" More generally this statement comes without explanation or rationale in the previous paragraph justifying this conclusion. If this statement is true, it should be further explained in dedicated paragraph.	To be clarified
17	ES	S.9.1	Further guidance should be provided to manufacturers to establish whether a "vulnerability" is "actively exploited". More precisely	Clarify the criteria to consider in order to establish that a vulnerability is "actively exploited".

			which criteria should be considered to establish that a vulnerability is "actively exploited"?	
18	ES	S.9.1	As per the CRA, the reporting obligation are not limited in time. Yet, it is not realistic to require manufacturers to fulfil their reporting obligations on products for ever. As such, this unlimited obligation in time will create ever growing costs, which will divert investment from the development of new products but rather support functions. Therefore a limit in time should be defined for the reporting obligations to provide clarity to manufacturer. A good approach would limit this obligation in time until the support period of the last product which has been placed on the market has expired.	Clarify that the reporting obligation applies until the support period of the last product which has been placed on the market has expired.
19	ES	S.9.1	After discussing with IT product security teams, it appears that the definitions of the two events to be reported as per article 14 i.e. "actively exploited vulnerability" and "severe incident having an impact on the security of the product with digital elements" are not exclusive to each other, meaning that an event could fall within the two categories at the same time. ➔ Was the intention of the legislator to designate two different types of events by using the wording “actively exploited vulnerability" and "severe incident having an impact on the security of the product with digital elements"? ➔ If yes, further guidance shall be provided to manufacturers regarding their delineation ➔ If not, 1. it shall be made clear within the guidance that these events may overlap, 2. the reporting process to apply in such case shall be clarified, and	Clarify the following: ➔ Was the intention of the legislator to designate two different types of events by using the wording “actively exploited vulnerability" and "severe incident having an impact on the security of the product with digital elements"? ➔ If yes, further guidance shall be provided to manufacturers regarding their delineation ➔ If not, 1. it shall be made clear within the guidance that these events may overlap, 2. the reporting process to apply in such case shall be clarified, and 3. the reporting of such event in the SRP shall be streamlined (i.e. allow to declare it both as "actively exploited vulnerability" and "severe incident having an impact on the security of the product with digital elements")

			3. the reporting of such event in the SRP shall be streamlined (i.e. allow to declare it both as "actively exploited vulnerability" and "severe incident having an impact on the security of the product with digital elements") However, to alleviate the burden of work for manufacturers and streamline reporting, we strongly suggest ensuring that "actively exploited vulnerability" and "severe incident having an impact on the security of the product with digital elements" are exclusive, so that an event is either classified as one or the other.	However, to alleviate the burden of work for manufacturers and streamline reporting, we strongly suggest ensuring that "actively exploited vulnerability" and "severe incident having an impact on the security of the product with digital elements" are exclusive, so that an event is either classified as one or the other.
20	ES	P.210	This paragraph seems to imply that reporting obligations apply as of September 11th, 2026, to product with digital elements placed on the market, regardless their date of placing on the market. Our understanding so far was that the reporting obligations would apply to any product with digital elements placed on the market from September 11th, 2026. This is a MAJOR change in the interpretation, that has a huge impact for manufacturers. In particular it will create a substantial amount of work for manufacturer to monitor PwDE placed on the market in the past. On the other hand, the other interpretation allows for a progressive ramp up of the burden of work for manufacturer, alongside the placing on the market of new PwDE.	Clarify that the reporting obligations apply to any Product with digital elements placed on the market from September 11th, 2026, onwards.
21	ES		Comment on other topic In case a manufacturer designs, develops or manufactures a product according to a customer needs/specifications or for a customer, it is unclear under which conditions the transaction will qualify as 1. the placing on the market of a "tailor made product" or 2. the subcontracting of the design, development or manufacturing of a product for which the customer is the	To be clarified

			manufacturer. What are the differences between 1. the placing on the market of a "tailor made product" and 2. the subcontracting of the design, development or manufacturing of a product for which the customer is the manufacturer? ➔ What are the key criteria for establishing the placing on the market of a "tailor made product"? ➔ What are the key criteria for establishing the subcontracting of the design, development or manufacturing of a product for which the customer is the manufacturer?	

About us

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

EUROSMART
The Voice of the Digital Security Industry

Square de Meeûs 35 | 1000 Brussels | Belgium