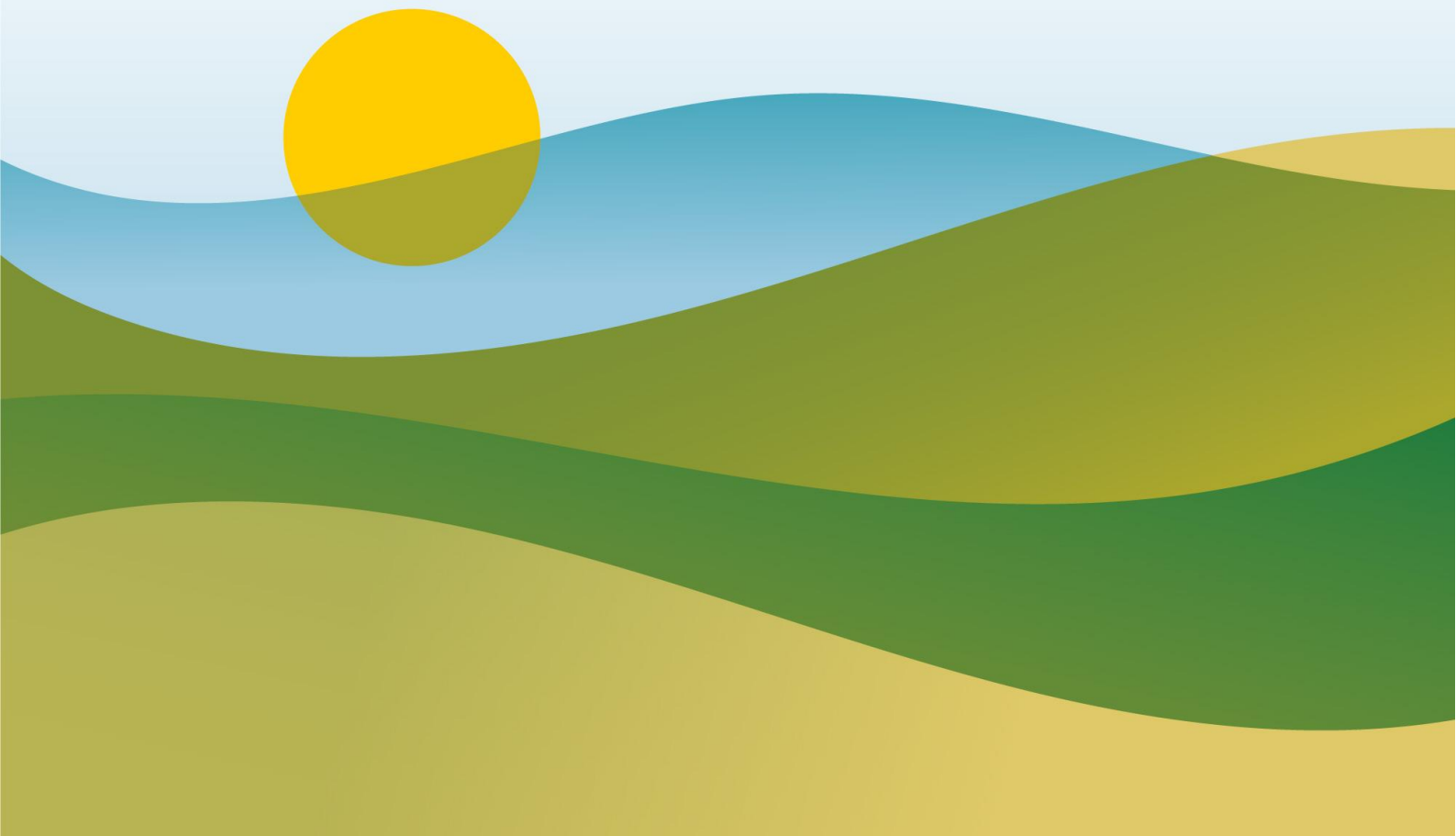
CEMA
European Agricultural Machinery Association

CEMA implementation guidance on the EU Cyber Resilience Act (CRA 2024/2847)

Version 1 - December 2025



Index

Goals of the document

This document aims to provide a CEMA interpretation of the EU Cyber Resilience Act (CRA), facilitate implementation for manufacturers, ensure consistency of such implementation within our sector, and serve as a basis for building CEMA positions externally and for standardisation work.

It is intended to support CEMA members in understanding and applying the CRA; it does not replace the applicable legislation, nor does it introduce any additional requirements. The interpretations provided are not legally binding and do not diminish the individual responsibility of manufacturers to ensure full compliance with the CRA. The document serves as an assistance tool only and may be updated as necessary.

Topic: Scope

Reference CRA	CRA 2024/2847 text	CEMA interpretation
Article 2	**Scope**	
Article 2 (1)	This Regulation applies to **products with digital elements made available on the market**, the **intended purpose** or **reasonably foreseeable use** of which includes a **direct or indirect logical** or **physical data connection** to a device or network.	The concept of "made available on the market" is available in the Blue Guide[1] 2022 §2.2. Assumption: All agricultural machinery falls within the scope of the CRA as it is made available on the market and requires CE marking, but Annex I (essential requirements) applies only to the "Electronic Information system" including software, hardware and remote data processing (if available) as per the relevant definitions. At least the intended purpose or the reasonably foreseeable use, as defined, must include a way to establish a data connection with the machinery from an external source, regardless the technology used (logical or physical). Examples of products in scope: - a USB port inside the machinery. - a ODB port inside the machinery. - a GPS connection. - a Bluetooth connection. - JTAG/Debug port of a microcontroller (see "Reasonably Foreseeable Use").

[1] https://single-market-economy.ec.europa.eu/news/blue-guide-implementation-product-rules-2022-published-2022-06-29_en

		Examples of products not in scope: - machine with no data connection at all. - a purely mechanical machine.
Article 2 (2)	This Regulation does not apply to products with digital elements to which the following Union legal acts apply: (a) Regulation (EU) 2017/745; (b) Regulation (EU) 2017/746; (c) Regulation (EU) 2019/2144.	The following products with digital elements are excluded: (a) Medical devices (b) In-vitro diagnostic medical devices (c) Type-Approved Vehicle Category *L, M, N, O
Article 2 (3)	This Regulation does not apply to products with digital elements that have been certified in accordance with Regulation (EU) 2018/1139.	Aviation exclusion.
Article 2 (4)	This Regulation does not apply to equipment that falls within the scope of Directive 2014/90/EU of the European Parliament and of the Council.	Naval exclusion.
Article 2 (5)	The **application** of this Regulation to products with digital elements covered by other Union rules laying down requirements that address all or some of the risks covered by the essential cybersecurity requirements set out in Annex I may be **limited or excluded** where: (a) such limitation or exclusion is consistent with the overall regulatory framework that applies to those products; and (b) the sectoral rules achieve the **same or a higher level of protection as that provided for by this Regulation**. The Commission is empowered to adopt delegated acts in accordance with Article 61 to supplement this Regulation by specifying whether such limitation or exclusion is necessary, the products and rules concerned, as well as the scope of the limitation, if relevant.	The CRA addresses all types of cybersecurity threats (e.g. H&S of the user, fraud, privacy, operational risks). Since no other regulation/s applicable to the AG industry achieves the same or a higher level of protection as that provided by the CRA, then the CRA applies in all cases.
Article 2 (6)	This Regulation does not apply to **spare parts** that are made available on the market to replace identical	Scenarios covered here: 1. Vehicle is still in production.

	components in products with digital elements and that are **manufactured** according to the same specifications as the components that they are intended to replace. [see also Recital (29)]: In order to ensure that products with digital elements made available on the market can be repaired effectively and their durability extended, an exemption should be provided for spare parts. That exemption should cover both spare parts that have the purpose of repairing legacy products made available before the date of application of this Regulation and spare parts that have already undergone a conformity assessment procedure pursuant to this Regulation.	2. Production has been discontinued, but it is still in support period. 3. Support period has ended. 4. Legacy products (machinery) (no longer produced and not compliant), spare parts for legacy products are excluded. Spare parts must be: 1. "identical" = "original": the parts are the same in every detail (e.g. features, functionalities, components) for them to comply with the CRA. *Example: Same Part Number – identical bill of materials*. 2. "manufactured according to the same specifications": the part may be manufactured by a third-party (under a legal agreement) or by the original manufacturer. *Example: the manufacturer starts to outsource the production of a component or changes the supplier for cost reasons.* 3. If a spare part needs a modification (e.g. due to obsolescence of a hardware component), it may no longer be considered identical. The machinery manufacturer must assess whether the modification constitutes a substantial modification and update the CRA technical documentation (e.g. bill of materials) accordingly to ensure the new component still qualifies as a spare part under the CRA. Note: If the spare part is manufactured or designed and manufactured by a third-party, they must inform the OEM in case a change is required (e.g., due to component discontinuation) in order to assess the machine compliance (see point 3).
Article 2 (7)	This Regulation does not apply to products with digital elements developed or modified exclusively for national security or defence purposes or to products specifically designed to process classified information.	National security / Defence exclusion.

Article 2 (8)	The obligations laid down in this Regulation shall not entail the supply of information the disclosure of which would be contrary to the essential interests of Member States' national security, public security or defence.	Not related to machinery.
Article 3	**Definitions**	
Article 3. point (1)	**'product with digital elements'** means a software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately;	1. The presence of remote data processing is not pre-requisite for a software or hardware product to be considered a product with digital elements. 2. If remote data processing is present, it falls within the scope of the risk assessment. 3. Software or hardware components that are not classified as spare parts according to the definition below, are considered products with digital elements when they are placed on the market separately.
Article 3. point (2)	**'remote data processing'** means data processing at a distance for which the software is designed and developed by the manufacturer, or under the responsibility of the manufacturer, and the absence of which would prevent the product with digital elements from performing one of its functions;	Assumption: In the context of machinery, the "product with digital elements" in the definition refers to the entire machine. The remote data processing is: 1. a software running in a hardware that is external (not assembled within) to the machinery, so operating at a distance, physically away from the machine. 2. A software that is able to receive and/or send data to the machinery. 3. The absence of capability listed in point 2 would prevent the machinery from performing one of its intended functions (i.e., an intended function defined by the manufacturer and/or included in the user manual and/or service manual). 4. The software mentioned in point 2 has been developed by the manufacturer or under the responsibility of the manufacturer or on behalf of the manufacturer (the CE marking of the machinery also covers the conformity of the remote data processing as well).
Article 3. point (4)	**'software'** means the part of an electronic information system which consists of computer code;	Assumption: In the context of machinery, the software refers to the computer code components able to run on the machinery's hardware (as per Article 3. point(5)), . This hardware is made by components that are

		physically assembled into the machinery at the time it is placed on the EU market.
Article 3. point (5)	**'hardware'** means a physical electronic information system, or parts thereof capable of processing, storing or transmitting digital data;	Assumption: In the context of machinery, the hardware is the physical part of the machinery's electronic information system which is made by components that are physically assembled into the machinery at the time it is placed on the EU market.
Article 3. point (6)	**'component'** means software or hardware intended for integration into an electronic information system;	1. A component placed on the market separately from the finished product is considered a product with digital elements and requires CE marking (see Article 3.point (1)). 2. A component integrated into a machine (integrated into the machinery's electronic information system) that is not placed on the EU market separately is not considered a standalone product with digital elements and does not need CE marking.
Article 3. point (7)	**'electronic information system'** means a system, including electrical or electronic equipment, capable of processing, storing or transmitting digital data;	An electronic information system is a system made by hardware and software components as defined in the relevant sections (see definitions of software, hardware, component definitions)
Article 3. point (8)	**'logical connection'** means a virtual representation of a data connection implemented through a software interface;	A logical connection is a software enabling digital data communication between software components. Example: - a software protocol (e.g. VPN, IP).
Article 3. point (9)	**'physical connection'** means a connection between electronic information systems or components implemented using physical means, including through electrical, optical or mechanical interfaces, wires or radio waves;	The definition is self-explanatory. Note: the definition is not restricted to connections between physical components.
Article 3. point (10)	**'indirect connection'** means a connection to a device or network, which does not take place directly but rather as part of a larger system that is directly connectable to such device or network;	The definition is self-explanatory.
Article 3. point (23)	**'intended purpose'** means the use for which a product with digital	The intended purpose provides a general high-level description of a product's function,

	elements is intended by the manufacturer, including the specific context and conditions of use, as specified in the information supplied by the manufacturer in the instructions for use, promotional or sales materials and statements, as well as in the technical documentation;	including conditions which can be reasonably foreseen. It is the end-use of the product. Example: The intended purpose of an agricultural combine harvester is to crop corn in the field with operational functions activated, or to drive on roads with operational functions deactivated.
Article 3. point (24)	**'reasonably foreseeable use'** means use that is not necessarily the intended purpose supplied by the manufacturer in the instructions for use, promotional or sales materials and statements, as well as in the technical documentation, but which is likely to result from reasonably foreseeable human behaviour or technical operations or interactions;	It can be part of the [instructions to the users] (Annex II) supplied by the manufacturer or/and it can be found in the technical documentation (Annex VII). It includes any potential use of readily available features, for example an existing physical port whose communication capability is not foreseen by the manufacturer (e.g. flashing the firmware through the ECU JTAG/Debug port).

In order to better understand the difference between 'reasonably foreseeable use' and 'reasonably foreseeable misuse', here is the definition of 'reasonably foreseeable misuse':

Article 3. point (25)	'**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;	A 'reasonably foreseeable misuse' is not specified either in the instructions to the user or in the technical documentation drawn up by the manufacturer. It refers only to behaviour that occurs outside the intended context of use and environment, and cannot be predicted based on user behaviour or product characteristics. A misuse is something that is considered unlikely or implausible from the user's point of view when following the instructions provided by the manufacturer. For example, if an attack requires highly advanced, specialised knowledge beyond what a typical user possesses, then it is considered a misuse.

Topic: Substantial modification

Article 3 point (30)	'**substantial modification**' means a change to the product with digital elements following its placing on the	A substantial modification is a change that: - adds or modifies a functionality in a way that impacts compliance with essential

	market, which affects the compliance of the product with digital elements with the essential cybersecurity requirements set out in Part I of Annex I or which results in a modification to the intended purpose for which the product with digital elements has been assessed;	cybersecurity requirements (i.e., introduces a new risk). - modifies the intended purpose of the final product (as per the definition of Intended Purpose). Furthermore: - For any change it is the responsibility of the modifier to perform an impact analysis that evaluates whether a change compromises compliance to the CRA's essential requirements. - The results of the impact analysis must be documented (e.g., update of the SBOM or Risk assessment) even if the change is not a substantial modification. - If the intended purpose is modified (as per the definition of the Intended Purpose), the existing compliance is no longer valid. - A new conformity assessment is always required if the change is a substantial modification. Please refer to the Blue Guide section 2.1 under "*Repairs and modifications to products*" for more information on the impact of a substantial modification on product compliance.

Topic: Important and Critical Products

Reference CRA	CRA 2024/2847 text	CEMA interpretation
Article 7 & related annexes	**Important products with digital elements**	
Article 7 (1)	1. Products with digital elements which have the **core functionality of a product** category set out in Annex III shall be considered to be important products with digital elements and shall be subject to the conformity assessment procedures referred to in Article 32(2) and (3). The integration of a product with digital elements which has the core functionality of a product category set out in Annex III shall **not in itself render the product in which it is integrated subject** to the	When a component that qualifies as an important product listed in the annex III is integrated into a finished product which, in itself is not an important product (because it does not have a core functionality as described in Annex III), the finished product does not adopt/take over the conformity assessment procedure of the component made for integration. If a finished product containing an Annex III Class I or Class II component is imported into the EU, and the component is not placed separately on the EU market but together with

	conformity assessment procedures referred to in Article 32(2) and (3).	the product, then the conformity assessment procedure of the finished product also covers the component. In such a case, the component does not have to be certified separately (CE mark). The manufacturer of the finished product must follow the technical specifications applicable to Annex III Class I or Class II products (or the relevant vertical harmonised standard) for that component. 'Core functionality' is defined by the manufacturer and refers to the essential, most fundamental purpose of the product, the reason why the customer purchases it. Understanding core functionality helps marketers communicate the product's value proposition effectively and align it with customer expectations. Certain components should instead be considered as features: these are specific functionalities or attributes that enhance the product's usability or value. Core functionality represents the reason for having such features in the first place. These features are not essential to the core functionality itself.
Annex III		The Annex III list of important products is exhaustive and can only be extended by delegated act.
Annex III Class I	14. Microcontrollers with security-related functionalities	This is a microcontroller with a built-in HSM to protect against logical attack.
Annex III Class II	4. Tamper-resistant microcontrollers	This is a microcontroller with a built-in HSM to protect against (logical and) physical attack.
Article 8 & related annexes	**Critical products with digital elements**	
Article 8 (1)	… Where no delegated acts as referred to in the first subparagraph of this paragraph have been adopted, products with digital elements which have the core functionality of a product category as set out in Annex IV shall be subject to the conformity assessment procedures referred to in Article 32(3).	This paragraph also targets products that fall within the scope of a cybersecurity scheme under the CSA 2019/881. It concerns products that are used in an essential entity of a highly critical sector (as defined in NIS2 2022/2555). The NIS2 applies to **entities**, not to products. When a component that qualifies as a critical product listed in Annex IV is integrated into a

		finished product which, by itself is not a critical product (because it does not have a core functionality as described in Annex IV), the finished product does not adopt/take over the conformity assessment procedure of the component made for integration.
Annex IV	1. Hardware Devices with Security Boxes	We understand that this is not within the scope for the components used in our industry. "Hardware Devices with Security Boxes" refers to a category of ICT (Information and Communication Technology) products that include physical security measures designed to protect against tampering and unauthorised access. These devices are often used in environments where data security is critical, such as financial services, government, and other high-security sectors. The security scheme EUCC (under reg. 2019/881) covers the "Hardware Devices with Security Boxes" which include ICT products within its scope. See link ENISA – Application of Attack Potential: Hardware Devices with Security Boxes: https://certification.enisa.europa.eu/publications/application-attack-potential-hardware-devices-security-boxes_en

Topic: OEM–Supplier Relationship

Article 13	**Obligations of Manufacturers**	
Article 13 (5)	For the purpose of complying with paragraph 1, manufacturers shall exercise **due diligence when integrating** components sourced from third parties so that **those components do not compromise the cybersecurity** of the product with digital elements, including when integrating components of free and open-source software that have not been made available on the market in the course of a commercial activity.	The manufacturer of the finished product (OEM) "*is responsible for selecting suitable products that make up the combination, and for putting the combination together in such a way that it complies with the provisions of the laws concerned, and for fulfilling all the requirements of the legislation in relation to the assembly*" (see Blue Guide: 2.1. Product coverage - The product scope in Union harmonization legislation). The term *combination* is interpreted as the integration of the components into the finished product. "*Manufacturers must choose components and parts in such a way that the finished product*

		itself complies." (See Blue Guide: 2.1. Product coverage - The product scope in Union harmonization legislation). The OEM's risk assessment determines which features are necessary and whether the component features offered are suitable for compliance. The supplier of the component must provide enough information for the integrator (OEM) to do his due diligence. The supplier of a component is responsible for the features provided, including vulnerability handling (see Part II of Annex I), either as stipulated in a contract or as a legal obligation when the component is first placed on the European market. The manufacturer of the finished product (OEM) remains responsible for the overall compliance of the finished product. This includes enabling the component's security features to ensure secure-by-default configuration of the finished product based on the supplier instructions (Annex II point 8 (f)) . <u>Case where the component must be CRA compliant:</u> Due diligence (see Recital 34) requires the OEM to select components with the needed security properties and verify whether the declaration of conformity of the component covers the CRA. The OEM must integrate and configure this component in the finished product in accordance with the supplier's instructions (see Annex II). <u>Case where the component falls under a contract and is not required to be CRA compliant:</u> If the component is made for integration and is not placed separately on the EU market, the OEM must ensure that the finished product, including the component, complies with the CRA. CE marking applies only at the finished product level, not at the component level. The sharing of responsibilities may be outlined in a contract.
Article 13 (6)	Manufacturers shall, upon identifying a vulnerability in a component, including in an open source-component, which is integrated in the product with digital elements report the vulnerability to the person or entity manufacturing or maintaining the component, and	When the manufacturer of the finished product identifies a vulnerability in a component, this must be communicated and will trigger a reaction from the supply chain. The vulnerability must then be addressed and remediated.

	address and remediate the Vulnerability in accordance with the vulnerability handling requirements set out in Part II of Annex I. **Where manufacturers have developed a software or hardware modification to address the vulnerability in that component, they shall share the relevant code or documentation with the person or entity**	If the supplier of a CRA-compliant component is no longer able to provide support within the defined support period (for example, because the supplier goes out of business), and no other legal entity assumes responsibility, the manufacturer of the final product becomes responsible for finding an appropriate solution. It is advisable that by contract, in such cases, all source code and necessary information are provided by the supplier to the manufacturer of the finished product, enabling the latter to carry out their own remediation. For free and open-source software components, or components sourced from outside the EU, the manufacturer of the finished product is always responsible for remediating any identified vulnerability.
Related recitals		
Recital (34)	**integrating components sourced from third parties in** products with digital elements during the **design and development phase**, manufacturers should, in order to ensure that the products are **designed, developed and produced** in accordance with the essential cybersecurity requirements set out in this Regulation, exercise **due diligence** with regard to those components, **including free and open-source software components that have not been made available on the market**. The **appropriate level of due diligence** depends on the nature and the level of cybersecurity risk associated with a given component, and should, for that purpose, take into account **one or more** of the following actions: verifying, **as applicable,** that the **manufacturer of a component has demonstrated conformity with this Regulation, including by checking if the component already bears the CE marking**; verifying that **a component receives regular security updates, such as by checking its security updates history**; verifying that **a component is free from**	The manufacturer of the finished product, which is a product with digital elements, must exercise due diligence to meet the essential cybersecurity requirements for integrated third-party components, including free and open-source software. Due diligence is performed by the manufacturer of the finished product (OEM) on components that are also products with digital elements, placed on the EU market. This non-binding recital suggests taking into account one or more of the following actions to achieve compliance: • Verifying – where applicable – component compliance by checking the CE marking, • Ensuring the capability for regular security updates, • Checking for vulnerabilities in publicly accessible vulnerability databases, • Conducting additional security tests, • Enabling component security features to ensure secure-by-default configuration of the finished product based on the supplier instructions. If the manufacturer of the finished product identifies a vulnerability, it must be communicated and will trigger a reaction from the supply chain.

	vulnerabilities registered in the European vulnerability database established pursuant to Article 12(2) of Directive (EU) 2022/2555 or other publicly accessible vulnerability databases; **or** carrying out **additional security tests**. The **vulnerability handling obligations** set out in this Regulation, which manufacturers have to comply with when placing a product with digital elements on the market and for the support period, **apply to products with digital elements in their entirety, including to all integrated components**. Where, in the exercise of due diligence, the manufacturer of the product with digital elements identifies a vulnerability in a component, **including in a free and open-source component**, it should **inform the person or entity manufacturing or maintaining the component**, address and remediate the vulnerability, and, where applicable, provide the person or entity with the applied security fix.	The vulnerability must be addressed and remediated. If the supplier of a CRA-compliant component can no longer provide support within the support period (for example, because the supplier goes out of business) and no other legal entity assumes responsibility, the manufacturer of the final product becomes responsible and must find a suitable solution. It is advisable that by contract, in such cases, all source code and necessary information are provided by the supplier to the manufacturer of the finished product, enabling the latter to carry out their own remediation. For free and open-source software components or components sourced from outside the EU, the manufacturer of the finished product is always responsible for remediating vulnerabilities.
Recital (64)	… Manufacturers should only be able to deviate from the essential cybersecurity requirements in relation to tailor-made products that are fitted to a particular purpose for a particular business user and **where both the manufacturer and the user have explicitly agreed to a different set of contractual terms**.	A "tailor-made product" is a product within the scope of this Regulation (subject to CRA compliance), including components made for integration into a finished product by an OEM (as a business user) and for which deviations from the CRA essential requirements may be contractually agreed. Note: Products developed through "co-design" between 2 or more economic operators are not considered "tailor-made products". Such components, made for integration and developed in "co-design", are excluded from the scope of the CRA. See also Blue Guide section 2.3 on the placement on the market: "*Sometimes products are manufactured following the placing of an order. An offer or agreement, concluded before the stage of manufacture has been finalized, cannot be considered as placing on the market (e.g. an offer to manufacture a product according to certain specifications agreed by the parties to the contract, where the product will only be manufactured and delivered at a later stage).*"

Related Annexes		
Annex I part 1 (2) (b)	On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall: … be made available on the market with a secure by default configuration, unless otherwise agreed between manufacturer and business user in relation to a tailor-made product with digital elements, including the possibility to reset the product to its original state;	For the final product the text is clear, but for the explanation on the secure-by-default configuration of components we refer to the Subtopic: **Responsibilities of the Supplier of Components**
Annex II	At minimum, the product with digital elements shall be accompanied by: … 8. detailed instructions or an internet address referring to such detailed instructions and information on: … (f) where the product with digital elements is intended for integration into other products with digital elements, the information necessary for the **integrator to comply with the essential cybersecurity requirements** set out in Annex I and the documentation requirements set out in Annex VII.	This concerns components that are placed separately from the finished product on the EU market. For such components, made for integration, the supplier must provide instructions for adequate integration of the component, allowing the manufacturer of the finished product to perform due diligence (see recital 34).

Topic: Responsibilities of the Supplier of Components

The Cyber Resilience Act (CRA) requires:

- A secure-by-default configuration (Annex I, Part I, point (2)(b)) when making products with digital elements available on the market.
- An appropriate level of cybersecurity based on the risks (Annex I, Part I, point (1)) during the design and production of products with digital elements.

The CRA definition of a "product with digital elements" also includes components, meaning that components fall within the scope of the CRA.

The following guidance is intended to help manufacturers (suppliers) of components made for the integration address **two key questions** related to the essential cybersecurity requirements mentioned above:

1. Can a supplier make available on the market a component made for integration that has a non-"secure-by-default configuration", in order to facilitate its integration into a final product by the OEM?
2. Can a supplier place on the market an off-the-shelf component (made for integration) with different assurance levels?

In relation to these discussions it must first be made clear what is meant by '*component for integration*' and '*final product*'.

- A **"component",** according to the CRA, is any software or hardware element that is **intended to be integrated** into a product with digital elements (PDE), and which has cybersecurity relevance. A **"component made for integration"** is therefore not intended to be placed on the market as a standalone customer-ready-to-use product (final product), but rather as a building block used by manufacturers of other products (business users). The end-user will only use the component as integrated in a final product.
- A **final product**[2]: means a standalone customer-ready-to-use product, so it is intended to be used directly by the end user (e.g. farmer).

1. Can a supplier make available on the market a component made for integration that has a non-"secure-by-default configuration", in order to facilitate its integration into a final product by the OEM?

The answer is YES.

The main justification is integrating components, which are already securely configured at the time of integration, is difficult and requires additional steps. This makes the integration of components unnecessarily complex and it could also expose extra attack surface during integration. Since the component does not present risks when used standalone, there is no need for security configuration prior to integration

Making components available on the market without a secure configuration significantly reduces this complexity as illustrated with following examples:

- An ECU that includes a crypto module is shipped without secret keys and with privileged functions disabled. The OEM can provision the keys and activate the security features during integration (without the need for authentication).
- An ECU that includes a Secure Boot feature and is delivered without the application (minimal bootloader only). The OEM can flash the application and provision the root of trust to activate secure boot, without disabling security or replacing the root of trust.

The main condition, with reference to Article 13 and Annex II, point 8(f), is that the supplier must provide "*information necessary for the integrator to comply with the essential cybersecurity requirements*".

If a component made for integration is made available on the market without being configured, the supplier must inform the OEM (manufacturer of the vehicle integrating the component) how to configure it securely so that the security features are properly activated. All security features,

[2] In the blue guide a component could be seen as a finished product, as the guide only talks about two conditions:

- Fully manufactured and ready for distribution.
- Entered into the supply chain (i.e., transferred to another party), marking its official entry to the EU market.

Therefore the term final product is used rather than finished product.

necessary based on the risk assessment done by the supplier, must be available on the component at the time of placing on the market.
These guidelines are in line with the purpose of the essential requirements to deliver the final product to the customer with a secure-by-default configuration.

2. Can a supplier place on the market an off-the-shelf component (made for integration) with different assurance levels?

The answer is yes.
Components made for integration are intended to be part of a final product. As both the component made for integration and the final product fall within the scope of the CRA, the security measures can be implemented at different levels of the architecture of this final product (e.g. at the component level or at a higher level in the final product).
For example, a component that handles security-relevant data could be isolated in a private network protected by a gateway. As such the gateway takes over the security. Therefore, the OEM should be able to find components on the market that implement different level of security or different assurance levels.
The obligation of compliance for every component, regardless of the operational environment and security architecture of the final products it is built into, may result in over-engineering of the component.
Our interpretation is that the CRA does allow components made for integration to be placed on the market with different assurance levels, which in extremis could mean that, as a possible outcome of the risk assessment, the component may not need any cybersecurity feature.
Suppliers of off-the-shelf components do not always know into which final products the components will be integrated. Therefore, the supplier must well document the following at the component level, to encompass the different operational environments of the final products in which the component may be used:

- Given that the final application of off-the-shelf components, including the operational environment of the final product, is not known, the supplier can only make assumptions on the **operational environment** (CRA Art. 13.3) within the boundaries of the component.
- The supplier must perform a risk assessment based on the intended purpose and reasonably foreseeable use[3] (CRA Art. 13.3) to determine the **assets to be protected**. The supplier can either apply appropriate mitigation measures to enable protection **OR** he must provide information on residual risks to allow the integrator to ensure protection.
- If the product is not a component made for integration, the CRA requires the manufacturer to "ensure the cybersecurity", raising the security level as appropriate.
- The **supplier must provide instructions** to the user outlining the "intended purpose", "the security environment", "essential functionalities and information about the security properties" (Annex II 4.), "any known or foreseeable circumstance, related to the use of the product with digital elements in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, which may lead to significant cybersecurity risks" (annex II 5.)
- When selecting the components made for integration, **the manufacturer** of a final product must **carefully review the documentation** provided by the supplier to ensure that he is

[3] For components with only one function these concepts are overlapping.

selecting the right component with the appropriate level of security to be integrated in his final product or subsystem.

- Once the component is selected, the manufacturer must **follow the information provided for proper configuration/integration** of the component and **validate the successful integration** of the component (**due diligence**).

Topic: Vulnerability handling process including support period

Article 3	**Definitions**	

Article 3(41)	'**exploitable vulnerability'** means a vulnerability that has the potential to be effectively used by an adversary under practical operational conditions;	'Exploitable vulnerability' means that:
		• an attack path exists and
		• the attack path can be exploited
		  ○ in a reasonable amount of time,
		  ○ considering the reasonably foreseeable use of the product (e.g. the product is not disassembled), and regardless of the knowledge / tools required to exploit it.
		Note: linked to the database of vulnerabilities (reported actively exploited vulnerabilities).

Articles 13-14	**Vulnerability handling/reporting during the support period**	
Article 14 (1)	A manufacturer shall **notify** any **actively exploited vulnerability** contained in the product with digital elements that it becomes aware of simultaneously to the CSIRT designated as coordinator, in accordance with paragraph 7 of this Article, and to ENISA. The manufacturer shall notify that actively exploited vulnerability via the single reporting platform established pursuant to Article 16.	Currently, there is no explicit requirement for manufacturers to proactively monitor actively exploited vulnerabilities, nor is it clearly defined how they should become aware of such vulnerabilities. However, from 11 December 2027, with the implementation of the vulnerability-handling requirements, manufacturers are expected to be able to assess whether any newly identified vulnerability is relevant to their products. Where relevant vulnerabilities are identified, manufacturers must take appropriate action, such as informing users, issuing security updates, or implementing other necessary mitigation measures. If the manufacturer becomes aware of an actively exploited vulnerability, they should submit a notification via the single reporting platform established by ENISA. The manufacturer is obliged to provide a single point of contact to report the vulnerability. (This tool is different from the EU Vulnerability Database and is, as of today, not known).

Article 13 (8)	Manufacturers shall ensure, when placing a product with digital elements on the market, and for the **support period**, that vulnerabilities of that product, including its components, are handled effectively and in accordance with the essential cybersecurity requirements set out in Part II of Annex I. Manufacturers shall determine the support period so that it reflects the length of time during which the product is expected to be in use, taking into account, in particular, reasonable user expectations, the nature of the product, including its intended purpose, as well as relevant Union law determining the lifetime of products with digital elements. When determining the support period, manufacturers may also take into account the support periods of products with digital elements offering a similar functionality placed on the market by other manufacturers, the availability of the operating environment, the support periods of integrated components that provide core functions and are sourced from third parties as well as relevant guidance provided by the dedicated administrative cooperation group (ADCO) established pursuant to Article 52(15) and the Commission. The matters to be taken into account in order to determine the support period shall be considered in a manner that ensures proportionality. Without prejudice to the second subparagraph, the support period shall be at least five years. Where the product with digital elements is expected to be in use for less than five years, the support period shall correspond to the expected use time.	Recommendation for our sector regarding the **support period**: Support period of minimum 10 years (OEM decision) given that both conditions below are fulfilled: • that manufacturers of integrated components providing core functions continue delivering information during that period, AND • that external factors affecting compatibility do not render updates impossible (e.g. obsolescence of the tool-chain, expertise). For the manufacturer to decide on the support period, he can also take into account possible changes in the operational environment during the lifetime of the product. Furthermore, update retention is 10 years, during which updates can still be downloaded and installed after their release. Argumentation: • Many agricultural tractors have longer lifetimes; however they are typically used at full capacity as the main tool for farmers only during the first years (up to 8 years).Afterwards they are often used as assistance vehicles. Tractors are produced in the highest numbers per type and are therefore expected to be the prime target for possible cyberattacks. • Relatively few agricultural machines or tractors are connected. Whereas smartphones typically get 100% over-the-air (OTA) updates, for agricultural machinery and tractors across the entire portfolio the real figure is around 20% OTA, with approximately 80% of updates delivered by dealers. Farms are not considered as important or essential entities under NIS2.

ABOUT CEMA

CEMA aisbl (www.cema-agri.org) is the association representing the European agricultural machinery industry. With 11 national member associations, the CEMA network represents both large multinational companies and numerous European SMEs active in the sector.

CEMA represents about 1,300 manufacturers, producing more than 450 different types of machines with an annual turnover of about €40 billion and 150,000 direct employees. CEMA companies produce a large range of machines that cover any activity in the field from seeding to harvesting, as well as equipment for livestock management.

For more information, please contact:

CEMA aisbl

European Agricultural Machinery Industry Association

Avenue de Tervueren 168

1150 Brussels

Tel. +32 2 706 81 73

secretariat@cema-agri.org