FAQs on the Cyber Resilience Act

The Cyber Resilience Act (Regulation (EU) 2024/2847) lays down rules for the making available on the market of products with digital elements to ensure their cybersecurity, essential cybersecurity requirements for the design, development and production as well as vulnerability handling processes, obligations for economic operators in relation to those products, and rules on market surveillance and enforcement.

This preliminary set of technical Frequently Asked Questions (FAQs), published approximately two years before the entry into application of the Cyber Resilience Act (CRA), is designed to assist stakeholders in the implementation of the CRA. The FAQs are not meant to cover exhaustively the scope of the CRA, but rather aim to address recurring questions that the Commission services have collected since the entry into force of the CRA. This is intended to be a 'living document' that will be updated as and when necessary.

This document is prepared by the Commission services and should not be considered as representative of the European Commission's official position. The replies to the FAQs do not extend in any way the rights and obligations deriving from applicable legislation nor introduce any additional requirement. The expressed views are not authoritative and cannot prejudge any future actions the European Commission may take, including potential positions before the Court of Justice of the European Union, which is competent to authoritatively interpret Union law.

The Commission is also working on guidance pursuant to Article 26 of the CRA, to be adopted in the coming months.

FAQ Version	Date	Changes
1.0	03/12/2025	New
1.1	TBC	Copyright notice; minor formatting issues

Contents

1 Scope

1.1 When is a product with digital elements in scope of the Cyber Resilience Act?

The CRA 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*" (Article 2(1)), with the exception of products with digital elements that are exempted from its scope, as set out in Article 2(2), 2(3) and 2(4).

Three cumulative elements help to understand if a product with digital elements is subject to the CRA:

- Whether it meets the definition of a product with digital elements (see also entry *1.2 What is a product with digital elements? Are stand-alone software or firmware products with digital elements?*);
- Whether it is made available on the market;
- Whether its intended purpose or reasonably foreseeable use include a direct or indirect logical or physical data connection to a device or network (see also *1.3 What is a direct or indirect logical or physical data connection to a device or network?* and *4.1.4 What are intended purpose and reasonably foreseeable use, and how do they affect the cybersecurity risk assessment?*).

1.2 What is a product with digital elements? Are stand-alone software or firmware products with digital elements?

A product with digital elements is defined as "*a software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately*" (Article 3(1)).

Remote data processing is defined as "*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"* (Article 3(2)).

Software is defined as "*the part of an electronic information system which consists of computer code*" (Article 3(4)).

Hardware is defined as "*a physical electronic information system, or parts thereof capable of processing, storing or transmitting digital data*" (Article 3(5)).

Electronic information system is defined as "*a system, including electrical or electronic equipment, capable of processing, storing or transmitting digital data*" (Article 3(7)).

A product with digital elements can take many forms, for example:

- Standalone software that can be downloaded and installed on a device, e.g. a mobile app that can be downloaded via an app store, or a program that can be downloaded via a website;
- Software intended for integration into an electronic information system, when placed separately on the market, e.g. firmware or software meant to be embedded into hardware devices;
- Software that is placed on the market together with a hardware product, whether pre-loaded on the hardware or not, e.g. the drivers that are necessary for a printer to work properly, the operating system in a laptop, or the tools used to design and program FPGAs;
- Various types of hardware, such as more foundational components (e.g. integrated circuits, motherboards; sensors); consumer devices (e.g. smartphones, laptops, smart fridges); complex devices (e.g. industrial IoT devices, machinery).

A product with digital elements also includes its remote data processing solutions.

As stated in Recital 12, websites that do not support the functionality of a product with digital elements are not themselves products with digital elements. Websites that support the functionality of a product with digital elements may fall in scope of the CRA to the extent that they meet the definition of remote data processing (Article 3(2)).

Similarly, services, such as standalone Software-as-a-Service (SaaS) or other cloud solutions designed and developed outside the responsibility of a manufacturer of a product with digital elements are not themselves products with digital elements. Where, on the other hand, such services meet the definition of remote data processing, they fall within the scope of the CRA.

The concept of remote data processing will be part of separate guidance.

1.3 What is a direct or indirect logical or physical data connection to a device or network?

A physical connection is defined as "*a connection between electronic information systems or components implemented using physical means, including through electrical, optical or mechanical interfaces, wires or radio waves*" (Article 3(9)).

A logical connection is defined as "*a virtual representation of a data connection implemented through a software interface*" (Article 3(8)).

An indirect connection is defined as "*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*" (Article 3(10)).

Under certain conditions, all products with digital elements integrated in or connected to a larger electronic information system can serve as an attack vector for malicious actors. As a result, even hardware and software considered to be less critical can facilitate the initial compromise of a device or network, enabling malicious actors to gain privileged access to a system or to move laterally across systems. Manufacturers should therefore ensure that all products with digital elements are designed and developed in accordance with the essential cybersecurity requirements laid down in this Regulation. That obligation relates to both products that can be connected physically via hardware interfaces and products that are connected logically, such as via network sockets, pipes, files, application programming interfaces or any other types of software interface. As cyber threats can propagate through various products with digital elements before reaching a certain target, for example by chaining together multiple vulnerability exploits, manufacturers should also ensure the cybersecurity of products with digital elements that are only indirectly connected to other devices or networks (Recital 9).

A physical connection can be direct, for example, when a product with digital elements connects via a USB cable (e.g. a printer connecting to a laptop); via an Ethernet cable (e.g. a PC connecting to a router); via a fibre optic cable (e.g. a fibre-optic router connecting to the internet service provider's network) or a copper cable (e.g. an industrial fieldbus such as PROFIBUS connecting a sensor to a programmable logic controller); via radio waves, such as via Wi-Fi (e.g. a point-of-sale (POS) terminal that connects to a shop's network), Bluetooth (e.g. a Bluetooth headset connecting to a smartphone), near-field communication technology (e.g. a door lock connecting to an NFC tag).

A logical connection can be direct, for example, when a product with digital elements initiates or manages communication with other devices or networks (e.g. a browser establishing an HTTPS session to access a website, or an email client initiating an IMAP or SMTP exchange); or it can be indirect, when a product with digital elements does not itself initiate the communication but runs on a host system that does (e.g. an offline text editor or a calculator that are indirectly connected via the operating system).

Products with digital elements can simultaneously have more than one form of data connection to other devices or networks.

On the other hand, a product with digital elements does not have a direct or indirect data connection when its intended purpose or reasonably foreseeable use do not include

such connection to other devices or networks. Some examples of products that would not fall in scope of the CRA include:

- a dishwasher with embedded firmware controlling dishwashing cycles, but with no capability to connect to other devices or networks;
- a basic calculator with embedded firmware performing arithmetic operations, but with no capability to connect to other devices or networks;
- an electronic toy with embedded firmware playing pre-recorded light and sound effects, but with no capability to connect to other devices or networks;
- a coffee machine with embedded firmware that sets brew times or coffee strength via a control panel, but with no capability to connect to other devices or networks
- an electric toothbrush with a wireless charging station, but with no capability to connect to other devices or networks.[1]

1.4 Does the CRA apply to products with digital elements placed on the market before 11 December 2027?

"Products with digital elements that have been placed on the market before 11 December 2027 are subject to the requirements of the CRA only if, from that date, they are subject to a substantial modification" (Article 69(2)).

"By way of derogation, the obligations laid down in Article 14 shall apply to all products with digital elements that fall within the scope of this Regulation, even if placed on the market before 11 December 2027" (Article 69(3)).

The CRA applies to products placed on the market before 11 December 2027 only if those products are substantially modified after that date. See also *7.1 When does the CRA start applying?*

For example, a manufacturer places on the market a smart TV in mid-2027. The manufacturer is not required to comply with the CRA for this product with digital elements. In 2028, it releases a software update, which does not qualify as a substantial modification, to fix a bug that causes apps running on the TV to crash after some usage time. The manufacturer is not required to bring the smart TV in conformity with the CRA, as it would not be substantially modifying it.

In 2029, that manufacturer releases a software update that qualifies as a substantial modification, for example because it modifies the original intended functions by enabling

[1] Firmware referred to in these examples may, however, fall in scope of the CRA when placed on the market separately.

the smart TV to control smart home systems. In that case, the manufacturer is required to bring the smart TV into compliance with the CRA.

See also *7.2 A manufacturer develops a product type before the CRA applies. Can it continue to manufacture products identical to that type after the CRA applies?*

A derogation to this general rule, however, applies to reporting obligations laid down in Article 14. Manufacturers are required to notify actively exploited vulnerabilities and severe incidents having an impact on the security of the product with digital elements for all products with digital elements falling within the scope of the CRA, including products that have been placed on the market before 11 December 2027 (Article 69(3)). See for further explanation *5.3 Does a manufacturer need to report actively exploited vulnerabilities or severe incidents for products placed on the market before the CRA* applies?

1.5 Are products that are manufacturer only for one's own use in scope of the CRA?

> *"Placing on the market is considered not to take place where a product is manufactured for one's own use"* (The 'Blue Guide' on the implementation of EU product rules 2022[2], section 2.3).

The CRA applies when a product with digital elements is placed on the market (and subsequent instances of making that product available). The Blue Guide on the implementation of EU product rules 2022 (henceforth, the Blue Guide) clarifies that placing on the market is not considered to take place when a product is manufactured for one's own use.[3]

For example, development and configuration tools developed by the manufacturer of a product with digital elements for its own use are not in scope of the CRA, unless they are placed on the market as separate products.

1.6 Can manufacturers release non-compliant versions of software for testing?

> *"Member States shall not prevent the making available on the market of unfinished software which does not comply with this Regulation, provided that the software is made*

[2] Commission notice - The 'Blue Guide' on the implementation of EU product rules 2022 (2022/C 247/01), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C:2022:247:FULL

[3] This is not the case where Union harmonisation legislation covers products manufactured for own use in its scope. The CRA, however, does not cover products manufactured for own use in its scope.

available only for a limited period required for testing purposes with a visible sign clearly indicating that it does not comply with this Regulation and that it will not be available on the market for purposes other than testing" (Article 4(3)).

Manufacturers can release non-compliant unfinished software for testing purposes, such as alpha versions, beta versions or release candidates, provided that that software is made available only for the time necessary to test it and gather feedback and that it is accompanied by a visible sign indicating its non-compliance.

Recital 37 further clarifies that "*manufacturers should ensure that software made available under those conditions is released only following a risk assessment and that it complies to the extent possible with the security requirements relating to the properties of products with digital elements laid down in this Regulation. Manufacturers should also implement the vulnerability handling requirements to the extent possible. Manufacturers should not force users to upgrade to versions only released for testing purposes*".

1.7 Can manufacturers maintain publicly accessible software archives?

"Manufacturers may maintain public software archives enhancing user access to historical versions. In those cases, users shall be clearly informed in an easily accessible manner about risks associated with using unsupported software" (Article 13(11)).

Manufacturers are allowed to maintain public software archives for historical versions of their products with digital elements that are no longer made available on the market. Users should be clearly informed of the risks that may stem from using software that is no longer supported.

1.8 Are products meant to be used for national security or defence purposes excluded from the CRA?

The CRA "*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*" (Article 2.7).

If a product with digital elements is not specifically and exclusively developed or modified for national security or defence purposes, or not specifically designed to process classified information, it falls under the scope of the CRA. So-called "dual-use" products that have both civilian and defence applications are therefore subject to the CRA when made available on the market, unless they are modified exclusively for national security or defence purposes.

Member States may subject products with digital elements that are in scope of the CRA to additional cybersecurity requirements for their procurement or use for specific purposes, provided that such requirements are consistent with Member States' obligations laid down in Union law and that they are necessary and proportionate for the achievement of those purposes, as foreseen by Article 5(1).

1.9 Are there products with digital elements covered by other Union legislation that are exempted from the CRA?

The CRA does not apply to products with digital elements:

- to which Regulation (EU) 2017/745 on medical devices and Regulation (EU) 2017/746 on in vitro diagnostic medical devices apply;
- to which Regulation (EU) 2019/2144 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users applies;
- certified in accordance with Regulation (EU) 2018/1139 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency; see also section *2.1 Regulation (EU) 2018/1139 on common rules in the field of civil aviation*.

The CRA also does not apply to equipment that falls within the scope of Directive 2014/90/EU on marine equipment; see also section *2.2 Directive (EU) 2014/90 on marine equipment*.

Delegated Regulation (EU) 2025/1535 also excludes from the application of the CRA products with digital elements that fall within the scope of Regulation (EU) No 168/2013 on the approval and market surveillance of two- or three-wheel vehicles and quadricycles, with the exception of L1e category vehicles designed to pedal.

2 Interplay with other legislation

2.1 Regulation (EU) 2018/1139 on common rules in the field of civil aviation

2.1.1 Are products falling within the scope of Regulation (EU) 2018/1139 also covered by the CRA?

Both the CRA and Regulation (EU) 2018/1139 (also known as the 'EASA Basic Regulation') establish rules for placing products on the market. The CRA applies to products with digital elements, while the EASA Basic Regulation applies to aeronautical products, parts, and equipment (including software).

The EASA Basic Regulation sets out essential requirements, including those for protection against information security threats, and mandates EASA certification of civil aircraft and related products in accordance with Implementing Regulation (EU) 748/2012, Part 21.

Since 2020, the European Union Aviation Safety Agency (EASA) has explicitly integrated information security aspects into its certification rules by amending several Certification Specifications and issuing new guidance.

On that basis, Article 2(3) of the CRA exempts products certified under Regulation (EU) 2018/1139 from its applicability.

However, products that fall within scope of Regulation (EU) 2018/1139 but that are not certified under that Regulation, such as drones in the open category (the majority of leisure drone activities and low-risk commercial activities), may be covered by the CRA (if they are products with digital elements and are made available on the market).

Also, where components are intended for integration into products certified under Regulation (EU) 2018/1139 but those components are not certified under that Regulation, those components may be covered by the CRA (if they are products with digital elements and made available on the market).

2.2 Directive (EU) 2014/90 on marine equipment

2.2.1 Are products falling within the scope of Directive (EU) 2014/90 also covered by the CRA?

The CRA and Directive (EU) 2014/90 both provide for rules for making available on the market certain products: for products with digital elements, and for marine equipment, respectively.

According to Article 2(4), the CRA does not apply to equipment that falls within the scope of Directive (EU) 2014/90.

Equipment that falls within the scope of Directive (EU) 2014/90 is listed in the annex to Commission Implementing Regulation (EU) 2025/1533 as regards design, construction and performance requirements and testing standards for marine equipment.

However, where components are intended for integration into equipment within the scope of Directive (EU) 2014/90 but those components do not fall within the scope of that Directive, those components may be covered by the CRA (if they are products with digital elements and made available on the market).

2.3 Product Liability Directive (EU) 2024/2853

2.3.1 What is the interplay between the CRA and the Product Liability Directive?

The CRA and the Product Liability Directive (PLD) are of a different nature and, while they complement each other, there is no legal overlap.

The PLD sets out liability rules for defective products so that injured persons can claim compensation when a damage has been caused by defective products. It establishes the principle that the manufacturer of a product is liable for damages caused by a defect in their product irrespective of fault or negligence (strict liability).

The defectiveness of the product is assessed based on whether the product provided the safety that one can expect, or that is required under Union or national law. The defectiveness must be assessed taking into consideration all circumstances, including cybersecurity requirements.

For example, the CRA provides for specific obligations for manufacturers regarding security updates for products with digital elements (Annex I).

Whilst the PLD does not impose any substantive obligation for manufacturers to update or upgrade the product, under the PLD the manufacturer remains liable for any defects introduced through an update or upgrade of the product after it has been placed on the market. Or, for any defects that arise after the product has been placed on the market due to the lack of an update or upgrade.

2.4 Machinery Regulation (Regulation (EU) 2023/1230)

2.4.1 What is the interplay between the CRA and the Machinery Regulation?

Manufacturers of products falling within the scope of Regulation (EU) 2023/1230 of the European Parliament and of the Council which are also products with digital elements as defined in this Regulation should comply with both the essential cybersecurity requirements set out in this Regulation and the essential health and safety requirements set out in Regulation (EU) 2023/1230. The essential cybersecurity requirements set out in this Regulation and certain essential requirements set out in Regulation (EU) 2023/1230 might address similar cybersecurity risks. Therefore, the compliance with the essential cybersecurity requirements set out in this Regulation could facilitate the compliance with the essential requirements that also cover certain cybersecurity risks as set out in Regulation (EU) 2023/1230, and in particular those regarding the protection against corruption and safety and reliability of control systems set out in sections 1.1.9 and 1.2.1 of Annex III to that Regulation. Such synergies have to be demonstrated by the manufacturer, for instance by applying, where available, harmonised standards or other technical specifications covering relevant essential cybersecurity requirements following a risk assessment covering those cybersecurity risks. The manufacturer should also follow the applicable conformity assessment procedures set out in this Regulation and in Regulation (EU) 2023/1230. The Commission and the European standardisation organisations, in the preparatory work supporting the implementation of this Regulation and of Regulation (EU) 2023/1230 and the related standardisation processes, should promote consistency in how the cybersecurity risks are to be assessed and in how those risks are to be covered by harmonised standards with regard to the relevant essential requirements. In particular, the Commission and the European standardisation organisations should take into account this Regulation in the preparation and development of harmonised standards to facilitate the implementation of Regulation (EU) 2023/1230 as regards in particular the cybersecurity aspects related to the protection against corruption and safety and reliability of control systems set out in sections 1.1.9 and 1.2.1 of Annex III to that Regulation. The Commission should provide guidance to support manufacturers subject to this Regulation that are also subject to Regulation (EU) 2023/1230, in particular to facilitate the demonstration of compliance with relevant essential requirements set out in this Regulation and in Regulation (EU) 2023/1230 (Recital 53 of the CRA).

The Machinery Regulation (MR) will apply from 20 January 2027. It sets out, in its Annex III, essential requirements on health and safety, addressing also cybersecurity risks that may have an impact on safety.

Both the CRA and the MR provide for rules for making available on the market certain products. While the CRA covers products with digital elements, the MR covers machinery and related products, subject to certain exceptions.

The CRA sets out essential cybersecurity requirements for products with digital elements in its Annex I. The MR sets out for machinery and related products, in its Annex III, essential health and safety requirements, addressing also cybersecurity risks that may have an impact on safety (i.e. Annex III, sections 1.1.9 and 1.2.1).

A product may be a product with digital elements within the meaning of the CRA as well as machinery or a related product within the meaning of the MR, at the same time. In those cases, there may be an interplay, as described in Recital 53 of the CRA, between the CRA and the MR with regards to the cybersecurity requirements, as mentioned above, and the conformity assessment procedures, as set out individually in both the CRA and the MR.

For example: a certain type of machinery within the meaning of the MR that can be used to e.g. package vegetables for supermarkets, may contain hardware and software to ensure its functioning. In that sense, the food packing machinery may also be a product with digital elements within the meaning of the CRA.

2.4.2 Should a product comply with both the CRA and MR cybersecurity requirements?

A product with digital elements within the meaning of the CRA, may be also machinery or a related product, within the meaning of the MR, at the same time. In such cases, such product will need to comply with the cybersecurity requirements of the CRA as well as those of the MR. The cybersecurity requirements set out in the CRA and the MR are of such a nature that compliance with the cybersecurity requirements of only one of the Regulations cannot be automatically considered to also fully satisfy those of the other Regulation.

However, as the cybersecurity requirements set out in the CRA and the MR may for some aspects address similar risks, compliance with the CRA could facilitate compliance with the requirements set out in the MR. Nevertheless, manufacturers of products falling within scope of both the CRA and the MR would have to demonstrate such potential synergies on the basis of a risk assessment and e.g. by relying, where available, on harmonised standards or other relevant technical specifications.

2.4.3 Should a manufacturer ensure the assessment of conformity for a product through the procedures set out in both the CRA and the MR?

Both the CRA and the MR provide for conformity assessment procedures for relevant products with digital elements (in Article 32 of the CRA) and machinery and related products (in Article 25 of the MR) respectively.

For a product with digital elements, within the meaning of the CRA, which is also a machine or related product, within the meaning of the MR, manufacturers will need to ensure the assessment of conformity through the procedures set out individually in both the CRA and the MR. The conformity assessment procedures set out in the CRA and the MR are of such a nature that the assessment of conformity on the basis of the procedure

in one instrument cannot automatically be considered as sufficient to also satisfy the procedure that is required to be followed as per the other instrument (see also Recital 53 of the CRA).

2.5 General Product Safety Regulation (EU) 2023/988

2.5.1 What is the interplay between the CRA and the General Product Safety Regulation?

The CRA and the General Product Safety Regulation (GPSR) both provide for rules for the making available on the market of products, but they have a different scope in terms of the products and aspects that they apply to and the requirements that they set. In terms of products in scope of the Regulations, while the CRA only applies to products with digital elements, the GPSR applies to all consumer products to the extent that there are no specific provisions with the same objective under Union law that regulate the safety of the products concerned. In terms of the requirements set by the Regulations, the CRA provides for cybersecurity requirements, while the GPSR provides safety requirements for products.

2.5.2 Does a product with digital elements need to comply with the requirements of both the CRA and the GPSR?

A product with digital elements may need to comply with both the requirements of the CRA and the GPSR. When a product with digital elements also poses other risks beyond cybersecurity risks that are covered by the CRA, those other risks may be regulated by other EU legislation such as the GPSR. As long as there is no product-specific regulation that regulates those other risks of the product with digital elements in question, the GPSR applies to the safety aspects of those risks (Article 11 CRA).

2.6 Radio Equipment Directive 2014/53/EU and the Commission Delegated Regulation (EU) 2022/30

2.6.1 What is the interplay between the CRA and the Radio Equipment Directive?

The CRA applies to the categories of radio equipment in scope of the Delegated Regulation (EU) 2022/30 adopted under the Radio Equipment Directive 2014/53/EU ('RED Delegated Regulation'). The CRA covers the essential requirements of the RED on Cybersecurity, which were rendered applicable via the RED Delegated Regulation as of 1 August 2025 and apply to the categories of radio equipment covered by the RED Delegated Regulation if placed on the market on or after 1 August 2025.

Technical standards have been requested for the purposes of the RED Delegated Regulation and are cited in the Official Journal of the European Union, in support of the corresponding essential requirements of the RED (EN 18031 series). To ensure legal clarity, the Commission aims to repeal the RED Delegated Regulation as of 11 December 2027[4].

In such a case, the categories of radio equipment specified in the RED Delegated Regulation, if placed on the market between 1 August 2025 and 10 December 2027, will be subject to the essential requirements of the RED on cybersecurity, which were rendered applicable via the RED Delegated Regulation. Conversely, if those products are placed on the market on 11 December 2027, or later, once the CRA has started to apply, those products will be subject to the essential requirements of the CRA.

A repeal of the RED Delegated Regulation, with effect from 11 December 2027, will not affect the Union market surveillance and control, under the Radio Equipment Directive 2014/53/EU, of the compliance of radio equipment with the essential requirements of the RED on cybersecurity, if that radio equipment was or is placed on the EU market between 1 August 2025 and 10 December 2027, and was subject to any of those essential requirements.

2.7 European Health Data Space Regulation (Regulation (EU) 2025/327)

2.7.1 What is the interplay between the CRA and the European Health Data Space Regulation?

The CRA and the European Health Data Space (EHDS) Regulation both provide rules for the making available on the market of products: the CRA provides for essential cybersecurity requirements for products with digital elements, while the EHDS Regulation provides, amongst other things, essential requirements, including interoperability and logging requirements, and further obligations to be complied with for Electronic Health Record (EHR) systems.

A product may be a product with a digital element within the meaning of the CRA and an EHR system within the meaning of the EHDS Regulation at the same time.

Example: A computer or a software that has been marketed and procured by a hospital designed for storing and viewing patient summaries while delivering healthcare services, could be a product with digital elements within the meaning of the CRA that is also an EHR system, within the meaning of the EHDS Regulation.

[4] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14766-Cybersecurity-repeal-of-Delegated-Regulation-supplementing-the-Radio-Equipment-Directive_en

2.7.2 Should a product comply with both the CRA and EHDS Regulation requirements?

A product may be a product with digital elements within the meaning of the CRA and an EHR system within the meaning of the EHDS Regulation at the same time. In such cases, a product will need to comply with the requirements set out in both the CRA and the EHDS Regulation (Recital 112 EHDS Regulation). The cybersecurity requirements set out in the CRA and the EHDS Regulation are of such a nature that compliance with the requirements of either the CRA or the EHDS Regulation alone will not fully satisfy those of the other Regulation.

However, the CRA (Article 13(4) CRA) determines that for products with digital elements that are also EHR systems, the cybersecurity risk assessment required by the CRA may be part of the risk assessment required by the EHDS Regulation.

2.7.3 Should a manufacturer ensure the assessment of conformity for a product through the procedures set out in both the CRA and EHDS Regulation?

Both the CRA and the EHDS Regulation provide for conformity assessment procedures for relevant products. In the case of the CRA this applies to products with digital elements, whereas under the EHDS Regulation this applies to the harmonised software components of EHR systems (as defined in Article 25(1) EHDS Regulation).

However, this does not mean that manufacturers need to ensure the assessment of conformity of the cybersecurity of a product through the procedures set out in both the CRA and the EHDS Regulation in cases where a product is a product with digital elements within the meaning of the CRA and an EHR system within the meaning of the EHDS Regulation at the same time. The CRA (Article 32(5a), which was introduced by the EHDS Regulation) determines that in such cases the conformity assessment procedure of the EHDS Regulation should apply instead of the procedure of the CRA.

2.7.4 Should the manufacturer draw up separate EU declarations of conformity per Union legal act?

Concerning the drawing up of the EU declaration of conformity by the manufacturer, Article 39(2) of the EHDS Regulation provides for a single EU declaration of conformity to be drawn up in respect of all Union legal acts applicable to the EHR system. That EU declaration of conformity shall contain all the information required for the identification of the Union legal acts to which it relates. The CRA provides the same for products with digital elements in Article 28(3).

2.8 General Data Protection Regulation (Regulation (EU) 2016/679)

2.8.1 What is the interplay between the CRA and the General Data Protection Regulation?

The CRA and the General Data Protection Regulation (GDPR) are of a different nature and there is no legal overlap. The CRA sets out obligations for economic operators making available products with digital elements on the market while the GDPR provides for rules, including obligations, for natural and legal persons acting as controllers or processors of personal data processing.

While of a different nature, these regulations may complement each other. The CRA provides for cybersecurity requirements for products with digital elements that may contribute to the protection of personal data of natural persons. These include amongst other things the confidentiality and integrity of personal and other data, data minimisation, a secure by default configuration as well as requirements relating to vulnerabilities handling and minimising the impact of significant incidents (Annex I). Similarly, the GDPR provides for requirements for personal data processing activities, such as data minimisation and data integrity and confidentiality principles (Article 5 GDPR), the obligation for data protection by design (Article 25 GDPR), data security (Article 32 GDPR), and the notification of personal data breaches (Article 33 GDPR), which may contribute to the cybersecurity of products with digital elements.

However, the manufacturer's compliance for a product with digital elements with the requirements of the CRA does not have any formal impact on the tools used by controllers or processors under the GDPR to demonstrate compliance of the processing of personal data with the GDPR (such as by means of codes of conduct (Article 40 GDPR) or certification schemes (Article 42 GDPR)).

2.9 Data Act (Regulation (EU) 2023/2854)

2.9.1 What is the interplay between the CRA and the Data Act?

The CRA and the Data Act (DA) are essentially of a different nature, with the former setting rules for the making available of products with digital elements on the market, while the latter lays down rules for (amongst other things) the making available of product data and related services data to other entities.

However, in certain cases the requirements of the CRA and the DA may be applicable to similar products. In certain cases, a product with digital elements within the meaning of the CRA may also be a connected product or a related service within the meaning of the DA.

For example, home appliances that contain hardware and software and can be connected to the internet for their functionality, such as a 'smart' refrigerator, may also collect data concerning their use and be able to communicate that product data via the

Internet. In that sense, the smart refrigerator may be a product with digital elements within the meaning of the CRA and a connected product within the meaning of the DA at the same time.

2.9.2 How do the requirements for products with digital elements under the CRA take account of the obligations to make data available to users or third parties under the Data Act?

The CRA determines inter alia that products with digital elements shall be made available on the market only where they meet certain cybersecurity requirements (Article 6). Manufacturers have to ensure that when placing products with digital elements on the market, they are designed, developed and produced in accordance with those requirements (Article 13). Manufacturers will have to carry out a risk assessment comprising an analysis of cybersecurity risks based on the intended purpose and reasonably foreseeable use of the product.

Where a product with digital elements within the meaning of the CRA may also be subject to the requirements of the DA to make data available to users or third parties (Articles 4 and 5 DA), the manufacturer will need to ensure that relevant requirements under the DA are also considered as part of the risk assessment. Manufacturers should keep in mind that while the DA obliges access to product and related service data to users and third parties, it also establishes measures for data holders to restrict or refuse data sharing in certain cases (e.g. using the so-called 'trade secret' and 'safety and security' handbrakes (Articles 4(8) and 5(11), and 4(2), DA respectively).

2.9.3 Should a manufacturer redesign their products to comply with the requirements of the DA and the CRA?

Under the DA, there is no strict (re)design product obligation. Rather, manufacturers remain free to design products as they see fit, as long as the obligations related to making data available are complied with.

Whilst the CRA is set to apply fully by 11 December 2027, products with digital elements placed on the market before that date are only subject to the CRA's cybersecurity requirements if, from that date, they are subject to a substantial modification (Article 69(2) CRA). Reporting obligations, e.g. for actively exploited vulnerabilities, apply for all products with digital elements (Article 14). See also *1.4 Does the CRA apply to products with digital elements placed on the market* before 11 December 2027?

3 Important and critical products

3.1 What determines if a product with digital elements is an important or critical product?

In accordance with Articles 7(1) and 8(1), a manufacturer should look at the core functionality of its product with digital elements to determine whether that product is an important or critical product with digital elements and is therefore subject to the corresponding conformity assessment procedures.

The technical descriptions of the categories of important and critical products with digital elements are laid down in Commission Implementing Regulation (EU) 2025/2392 of 28 November 2025 on the technical description of the categories of important and critical products with digital elements.

3.2 Does integrating an important or critical product with digital elements into another product with digital elements render that product important or critical?

As specified in Article 7(1), integrating an important or critical product with digital elements into another product with digital elements does not automatically render that product subject to the conformity assessment procedures applicable to important and critical products. For example, integrating an embedded browser as a component of a news app for use in smartphones does not in itself render the news app subject to the conformity assessment procedure applicable to products with digital elements that have the core functionality of "standalone and embedded browsers". Similarly, integrating a secure element into a laptop does not in itself render the laptop subject to the conformity assessment procedure applicable to products with digital elements that have the core functionality of "smartcards and similar devices, including secure elements".

As stated in *3.1 What determines if a product with digital elements is an important or critical product?*, the core functionality of the product with digital elements into which other components are integrated determines whether that product is an important or critical product with digital elements.

3.3 Does the classification of a product as important or critical impact the manufacturer's risk assessment?

In accordance with paragraphs (1) to (3) of Article 13, the CRA establishes that manufacturers of products with digital elements are to implement the essential cybersecurity requirements in a way that is proportionate to the risks of the product with

digital elements, based on the intended purpose and reasonably foreseeable use as well as the conditions of use of the product with digital elements, taking into account the length of time the product is expected to be in use. Irrespective of whether the product with digital elements is considered to be an important or critical product with digital elements, manufacturers are to carry out a comprehensive cybersecurity risk assessment and indicate how the essential cybersecurity requirements are implemented as informed by the risk assessment, including their testing and assurance.

For example, a manufacturer wishes to place on the market two different versions of a VPN. In accordance with its risk assessment, the manufacturer determines that one of the two VPNs presents more substantial risks, for example because that VPN is intended to be deployed in a critical infrastructure environment, while the other VPN presents fewer risks, for example because it is intended only for use in a residential setting. Consequently, the manufacturer is expected to implement the essential requirements for both products in such a way that it ensures that the respective risks are mitigated accordingly.

3.4 Does the presence of multiple functions mean that a product does not have the core functionality of an important or critical product?

As explained in Recital 4 of Commission Implementing Regulation (EU) 2025/2392 of 28 November 2025 on the technical description of the categories of important and critical products with digital elements, the fact that a product with digital elements performs functions other than or additional to its core functionality does not in itself mean that the product with digital elements does not have the core functionality of an important or critical product. For example, products that have the core functionality of “operating systems” (an important product with digital elements of Class I) often include software that performs ancillary functions not included in the technical description of that product category, such as calculators or simple graphics editors. Products with digital elements often also incorporate components that have the functionality of another important or critical product with digital elements, such as an operating system integrating browser functionality, or a router integrating firewall functionality. This, however, does not in itself mean that such products with digital elements do not have the core functionality of “operating systems” or “routers, modems intended for the connection to the internet, and switches” (also important products with digital elements of Class I), respectively.

On the other hand, a product that has the ability to perform the function(s) of an important or critical product category but whose core functionality itself is different from that of such product category is not to be considered to have that core functionality. For example, a security orchestration, automation and response (SOAR) software often has the ability to perform the functions of “security information and event management (SIEM) systems”. However, as the SOAR’s core functionality is different from that of a

SIEM, SOAR software is generally not to be considered to have the core functionality of “security information and event management (SIEM) systems”. Similarly, a smartphone typically integrates components that perform the functions of several important or critical products, such as an operating system or an integrated password manager. However, as a smartphone’s core functionality is not that of an operating system or of a password manager, it is generally not to be considered to have the core functionality of an operating system or of a password manager.

4 Manufacturer's obligations

4.1 Risk-based approach and risk-assessment

4.1.1 What does the CRA require of the manufacturer's cybersecurity risk assessment?

Union harmonisation legislation related to products made available on the internal market and based on the New Legislative Framework (NLF)[5] typically requires manufacturers to carry out a risk assessment, on the basis of which they need to implement the relevant essential requirements defined in the relevant legislation (see for instance section 4.1.1 of the Blue Guide). Those risk assessments are important documentation for the manufacturers to demonstrate (i.e. to market surveillance authorities) that they have implemented adequate requirements. Manufacturers may carry out a single risk assessment covering the needs of different legislations, or they may carry out individual risk assessments for each legislation separately. While it is up to the manufacturer to structure their risk assessment activities, they must be in a position to demonstrate compliance with each individual legislation. In accordance with the definition of product with digital elements (Article 3(1)), the manufacturer's cybersecurity risk assessment needs to cover the entire product with digital elements, including remote data processing when in scope and any supporting functions that may form part of the product with digital elements to be placed on the market.

Article 13(2) requires manufacturers to undertake an assessment of the cybersecurity risks associated with a product with digital elements and take the outcome of that assessment into account during the planning, design, development, production, delivery and maintenance phases of the product with digital elements with a view to minimising cybersecurity risks, preventing incidents and minimising their impact, including in relation to the health and safety of users. Thus, it is important to note that the cybersecurity risk assessment covers not only the initial stages of risk identification, risk analysis and risk evaluation during the design and development phases, but also the risk treatment measures implemented through the production, delivery and maintenance phases. Furthermore, this obligation applies to manufacturers of all products with digital elements within the meaning of the CRA, irrespective of whether the product with digital elements is in the "default category", an important or a critical product.

[5] The New Legislative Framework consists of Regulation (EC) 765/2008 setting out the requirements for accreditation and the market surveillance of products; Decision 768/2008 on a common framework for the marketing of products; and Regulation (EU) 2019/1020 on market surveillance and compliance of products.

In accordance with Article 13(3), the cybersecurity risk assessment shall indicate whether and, if so in what manner, the security requirements relating to the properties of products (set out in Part I, point (2), of Annex I) are applicable to the relevant product with digital elements, and how those requirements are implemented as informed by the cybersecurity risk assessment. It shall also indicate how the manufacturer has planned, designed, developed, produced, delivered and maintained the product with digital elements in such a way that they ensure an appropriate level of cybersecurity based on the risks (Part I, point (1), of Annex I) and the vulnerability handling requirements (set out in Part II of Annex I).

4.1.2 Does the CRA mandate a specific risk assessment methodology?

The CRA does not mandate a specific cybersecurity risk assessment methodology. The manufacturers can decide on the methodology they use to identify and treat the relevant risks. Manufacturers need to address all relevant risks emerging from the cybersecurity risk assessment, and the risk assessment methodology should therefore support manufacturers in documenting that this has been done (in accordance with Article 13(3)), allowing market surveillance authorities to verify how risks have been identified, evaluated and mitigated.

When modelling threat scenarios, manufacturers should ensure the use of a threat modelling methodology that appropriately reflects the threats and resulting risks associated to the product's intended purpose and reasonably foreseeable use. For instance, whereas products intended for use in critical infrastructure may be required to treat risks related to nation-state actors and advanced persistent threats, products intended for private consumer use typically have a lower risk profile and may use a different threat model. In this way, manufacturers can cover all relevant risks to a product in their risk assessment.

4.1.3 Does a manufacturer need to implement all the essential requirements?

Manufacturers need to comply with all essential cybersecurity requirements related to vulnerability handling (set out in Part II of Annex I) throughout the product's support period. However, with regards to essential cybersecurity requirements related to the product properties (set out in Part I of Annex I), manufacturers need to determine on the basis of the cybersecurity risk assessment which of those requirements are relevant for the type of product with digital elements concerned. In accordance with Article 13(4), where certain essential cybersecurity requirements are not applicable to a product with digital elements, the manufacturer should include a clear justification in the

cybersecurity risk assessment included in the technical documentation. This could be the case where an essential cybersecurity requirement is incompatible with the nature of a product with digital elements (see recital 55), or where no risks exist that require a mitigation in relation to that essential requirement.

For example, a product might not need to incorporate any specific mitigation measures related to the protection of personal data if the product's intended purpose and reasonably foreseeable use do not include the processing of any kind of personal data. In such cases, the product might still have the technical capability to process some kinds of personal data, but such use would not be included in the intended purpose and reasonably foreseeable use declared by the manufacturer. Where the product's technical capability to process personal data may lead to significant cybersecurity risks in the case of reasonably foreseeable misuse, the information and instructions to the user may need to include this information, in accordance with point 5 of Annex II of the CRA.

For example, as stated in recital 55, the intended purpose of a product with digital elements may require the manufacturer to follow widely recognised interoperability standards even if its security features are no longer considered to be state of the art. Similarly, other Union law requires manufacturers to apply specific interoperability requirements. Where this is the case, having the effect that an essential cybersecurity requirement is not applicable to a product with digital elements, but the manufacturer has identified cybersecurity risks in relation to that essential cybersecurity requirement, it should take measures to address those risks by other means, for instance by limiting the intended purpose of the product to trusted environments and/or by informing the users about those risks.

4.1.4 What are intended purpose and reasonably foreseeable use, and how do they affect the cybersecurity risk assessment?

In accordance with Article 13(2), the assessment of cybersecurity risks shall be carried out with a view to minimising such risks, preventing incidents and minimising their impact, including in relation to the health and safety of users. Furthermore, Article 13(3) clarifies that the analysis of cybersecurity risks shall consider at least the intended purpose and reasonably foreseeable use, as well as the conditions of use of the product with digital elements, such as the operational environment or the assets to be protected, taking into account the length of time the product is expected to be in use. As an example, manufacturers of hardware or software components used by many other products downstream may consider when the intended purpose and reasonably foreseeable use includes integration of those components. In those cases, the manufacturer must ensure relevant risks are duly treated (Article 13(1) and (2)), and

communicate to the users clear, understandable, intelligible and legible instructions that allow for the secure installation, operation and use of the product with digital elements (as per Article 13(8)).

Article 3(23) defines 'intended purpose' as the use for which a product with digital 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. Furthermore, 'reasonably foreseeable use' is defined in Article 3(24) as 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.

Where relevant to the intended purpose and reasonably foreseeable use, the manufacturer should also consider how downstream integration and end-use can affect the cybersecurity risk assessment (i.e. the specific context and conditions of use). Furthermore, manufacturers should inform their users, be they integrators, professional owners, or operators, consumers or others, through the information and instructions to the user about any assumptions or requirements that are needed for the secure installation, operation and use of the product with digital elements, in accordance with Article 13(18).

As stated in section 2.8 of the Blue Guide, manufacturers have to consider the conditions of use which can be reasonably foreseen prior to placing a product on the market, notably when such use could result from lawful and readily predictable human behaviour. This means manufacturers have to look beyond what they consider the intended use of a product and place themselves in the position of the average user of a particular product and envisage in what way they would reasonably consider using the product. For instance, as stated in section 3.1 of the Blue Guide, a tool designed and intended to be used by professionals only (such as an industrial IoT sensor or virtual private network), might eventually also be used by non-professionals; consequently, the design and instructions accompanied must take this possibility into account. Similarly, information necessary for the secure installation should still be provided in a way which is clear, understandable, intelligible and legible given the intended audience who is expected to carry out the installation, in accordance with Article 13(18). If the product can be easily accessible and is likely to be used by consumers, the manufacturer should consider the needs and risks of those consumers, such as through appropriate information and instructions to the users, including instructions for the secure installation, operation and use of the product with digital elements).

However, as set out in section 2.8 of the Blue Guide, not all risks can be prevented by product design, so intended or foreseeable deployment conditions should also be

considered. Where relevant, the cybersecurity risk assessment should take into account other measures that may be put in place by intended or foreseeable category of user (e.g. professional). For instance, the supervision and assistance of the intended users should be considered as part of the conditions which can be reasonably foreseen for products to be installed and used within certain professional settings, such as an industrial plant. As another example, some professional machine tools are intended for use by averagely skilled and trained workers under the supervision of their employer; the responsibility of the manufacturer cannot be engaged if such machine tools are rented by a distributor or third-party service-provider for use by unskilled and untrained consumers. Furthermore, it may in some cases be reasonable for the manufacturer to allow through the design of the product that the user can alter the product's configurations, removing security functionality or downgrading security measures to ensure legacy compatibility. In such cases, the manufacturer should include the relevant cybersecurity risks in their cybersecurity risk assessment, implement specific treatment measures covering those risks, and accompany those usage possibilities with appropriate information and instructions to the user to ensure secure deployment and that required security outcomes can be achieved. In addition, where this circumstance may lead to significant cybersecurity risks, the manufacturer should explicitly mention those risks in accordance with point 5 of Annex II of the CRA.

4.1.5 What is reasonably foreseeable misuse, and how does it affect the cybersecurity risk assessment?

In accordance with Article 13(18), the manufacturer should provide information to the users regarding the expected conditions for secure deployment and integration of the product. On their part, user should take into consideration the lawful conditions of use of the product defined by the manufacturer, provided these are reasonable and appropriate to the intended purpose and reasonably foreseeable use, in particular where low-skilled or vulnerable users are concerned. Article 3(24) defines 'reasonably foreseeable misuse' as 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. For instance, if the information and instructions to the user mentions that the product must be deployed on a secure network, deploying it on an insecure network might constitute a reasonably foreseeable misuse. Similarly, although some users might be hacking their devices for fun (or for security research), this use is not necessarily in line with the manufacturer's

stated intended purpose and reasonably foreseeable use, and therefore would constitute a form of misuse.[6]

Furthermore, manufacturers shall ensure that products with digital elements are accompanied by the information and instructions to the user set out in Annex II, including 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. Risks concerning reasonably foreseeable misuse must also be communicated in the information and instructions to the user. For instance, where the information and instructions to the user mentions that the product must be deployed on a secure network, this implies that the manufacturer may not have covered certain risks emerging from use on insecure networks. The manufacturer should therefore inform the user wherever such reasonably foreseeable misuse may still lead to significant cybersecurity risks.

4.1.6 How does the length of time the product is expected to be in use affect the manufacturer's cybersecurity risk assessment?

For the purpose of ensuring the security of products with digital elements after their placing on the market, manufacturers should determine the support period, which should reflect the time the product with digital elements is expected to be in use. Thus, in accordance with Article 13(3), the analysis of cybersecurity risks by the manufacturer shall take into account the length of time the product is expected to be in use (Article 13(8)). The manufacturer should also consider the product's lifetime in the design and development stage, and in particular should prepare the product to ensure that throughout the support period 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. Furthermore, according to Article 13(7) the risk assessment shall be documented and updated as appropriate during the product's support period. Where the risk assessment relies on the information and instructions to the users to address certain risks, such information and instructions to the users should be updated accordingly.

[6] As stated in Recital 75, Member States should aim to address, to the extent possible, the challenges faced by vulnerability researchers, including their potential exposure to criminal liability, in accordance with national law. Given that natural and legal persons researching vulnerabilities could in some Member States be exposed to criminal and civil liability, Member States are encouraged to adopt guidelines as regards the non-prosecution of information security researchers and an exemption from civil liability for their activities.

As an example, the manufacturer may consider reasonable projections about changes in the threat landscape and how these might impact the risk assessment throughout the product lifetime.

4.1.7 What is the relationship between harmonised standards and the manufacturer's cybersecurity risk assessment?

As stated in the Blue Guide, harmonised standards do not replace legally binding essential requirements. A technical specification given in a harmonised standard is not an alternative to a relevant essential or other legal requirement but only a possible technical means to comply with it. In risk-related harmonisation legislation this means in particular that manufacturers always, even when using harmonised standards the references of which are published in the Official Journal of the European Union ("OJ"), remain fully responsible for assessing all the risks of their product in order to determine which essential (or other) requirements are relevant. After this assessment a manufacturer may then choose to apply technical specifications given in harmonised standards the references of which are published in the OJ to implement 'risk reduction measures' which are specified by harmonised standards. In risk-related harmonisation legislation, harmonised standards the references of which are published in the OJ most commonly provide certain means to reduce or remove risks, while manufacturers remain fully responsible for the risk assessment to identify relevant risks and to identify relevant essential requirements, in order to select suitable harmonised standards the references of which are published in the OJ or other specifications.

Thus, even where the manufacturer uses a harmonised standard (where its reference is published in the OJ and which aims to cover certain risks) to satisfy essential requirements, the cybersecurity risk assessment has to be carried out and they must check whether the harmonised standard covers all risks of the product. In accordance with Article 27, where a manufacturer correctly applies a harmonised standard the reference of which is published in the OJEU which covers all the risks relevant to the product with digital elements, the product benefits from the presumption of conformity.[7]

As stated in Article 27(1) of CRA and section 4.1.2.2 of the Blue Guide, where a harmonised standard covers only part of the essential requirements identified as relevant by manufacturers or only certain aspects thereof, they additionally have to use other relevant technical specifications or develop solutions in accordance with general engineering or scientific knowledge laid down in engineering and scientific literature in order to meet the essential requirements of the CRA. In a similar way when manufacturers choose not to apply all the provisions given in a harmonised standard,

[7] As stated in footnote 179 of the Blue Guide.

and which normally would provide presumption of conformity, they need, on the basis of their own cybersecurity risk assessment, to indicate in their technical documentation how the compliance is reached or that relevant essential requirements are not relevant for the product.

The CRA standardisation request requests the development of a set of harmonised standards that are intended to provide either horizontal or product-specific information to manufacturers to support their compliance with the CRA. See also *6.10 When will harmonised standards to support CRA compliance be ready?*

4.1.8 What does a manufacturer need to include regarding the cybersecurity risk assessment in the technical documentation to be kept at the disposal of market surveillance authorities?

Article 13(12) and Article 31 require the manufacturer to draw up technical documentation containing information to demonstrate the conformity of the product to the applicable requirements, regardless of the conformity assessment procedure. This documentation may be part of the quality system documentation where the manufacturer chooses a conformity assessment procedure based on a quality system, in line with article 32. This is the case for conformity based on full quality assurance based on module H (part IV of CRA Annex VIII). The technical documentation must be available when the product is placed on the market, whatever its geographical origin or location. In accordance with Article 13(4), when placing a product with digital elements on the market, the manufacturer shall include the cybersecurity risk assessment in the technical documentation required pursuant to Article 31 and Annex VII. After placement on the market the manufacturer shall systematically document, in a manner that is proportionate to the nature and the cybersecurity risks, relevant cybersecurity aspects concerning the products with digital elements, including vulnerabilities of which they become aware and any relevant information provided by third parties, and shall, where applicable, update the cybersecurity risk assessment of the products. In particular, as part of the vulnerability handling requirement in Annex I, part 2(3), the manufacturer must update the risk assessment after the application of regular tests and reviews, wherever relevant information pertaining to the cybersecurity of the product emerges from such tests and reviews.

According to section 4.3 of the Blue Guide, in the case where a product has been subject to re-designs and re-assessments of the conformity, the technical documentation must reflect all versions of the product; describing the changes made, how the various versions of the product can be identified and information on the various conformity assessment.

In accordance with Article 53, where necessary to assess the conformity of products with digital elements and the processes put in place by their manufacturers with the essential cybersecurity requirements set out in Annex I, the market surveillance authorities shall, upon a reasoned request, be granted access to the data, in a language easily understood by them, required to assess the design, development, production and vulnerability handling of such products, including related internal documentation of the relevant economic operator.

4.2 Product-related essential requirements (Annex I, Part I)

4.2.1 Which technical measures does a manufacturer need to implement?

The CRA establishes a set of essential cybersecurity requirements relating to the properties of products with digital elements. Such requirements are objective-oriented and technology-neutral and apply horizontally to all products with digital elements.

The specific technical implementation of the essential requirements is dependent on the cybersecurity risk assessment that each manufacturer is required to undertake and take into account during the planning, design, development, production, delivery and maintenance phases of the product with digital elements, in accordance with Article 13(12). For further information on the risk assessment, see the section *4.1 Risk-based approach and risk-assessment*.

The manufacturer is required to detail in its technical documentation the means used to ensure that the product complies with the essential cybersecurity requirements, including instances where certain essential cybersecurity requirements are not applicable to the product with digital elements, in accordance with Article 13(4).

In order to facilitate the assessment of conformity with the essential requirements, the Commission adopted a standardisation request addressed to CEN, CENELEC and ETSI (the European Standardisation Organisations), requesting the development of harmonised standards in the technical areas covered by the CRA.

The CRA Standardisation Request requests, *inter alia,* the development of horizontal harmonised standards covering the product-related essential requirements laid down in Annex I, Part I of the CRA, with a view to support "*(i) the development of further, granular vertical harmonised standards for specific products or product types, and (ii) [to] support manufacturers in defining and implementing the security requirements applicable to their respective products, including particularly for products not covered by existing or planned vertical standards"* (Annex II, section 2.1 of CRA SR). For more information, see *6.10 When will harmonised standards to support CRA compliance be ready?*

It should be noted that the use of harmonised standards is voluntary. Manufacturers may demonstrate conformity with the essential requirements via other technical means and are required to document them in their technical documentation.

4.2.2 How can a manufacturer ensure that a product is free from all vulnerabilities?

> *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 without known exploitable vulnerabilities* (Annex I, Essential requirement (2)(a))
>
> *'vulnerability' means a weakness, susceptibility or flaw of a product with digital elements that can be exploited by a cyber threat* (Article 3(40)
>
> *'exploitable vulnerability' means a vulnerability that has the potential to be effectively used by an adversary under practical operational conditions* (Article 3(41)

The CRA does not require manufacturers to ensure that a product is free from all vulnerabilities.

The CRA requires manufacturers, at the moment of placement on the market, to ensure that, on the basis of their cybersecurity risk assessment and where applicable, the product does not contain known exploitable vulnerabilities.

In fact, not all vulnerabilities are exploitable under practical operational conditions. Some vulnerabilities can only be exploited in theoretical conditions (e.g. in a lab or in a simulation) and/or not under conditions which would occur in the operational environment of a given product with digital elements. Whether a vulnerability is exploitable needs to be addressed on a case-by-case basis, depending on the specific operational and technical conditions, including for example the extent to which the vulnerable code is invoked or loaded when the product is in use; the level and type of access required to carry out the exploit; whether compensating controls are already in place to mitigate exploitation.

For example, a smartphone may have a vulnerability that would enable an attacker to bypass security (e.g. skipping password checks); but in order to achieve this, the attacker needs physical access to the device and invasive physical tampering (e.g. using of a laser to cause a glitch) to make use of the exploit. On the basis of its risk assessment, the manufacturer may conclude that this would not be considered an exploitable vulnerability because it could not reasonably be exploited in practical operational conditions.

4.2.3 How should manufacturers deal with known exploitable vulnerabilities discovered after a product has been placed on the market but before reaching its final user?

Products with digital elements may be placed on the market and enter the distribution chain some time before they reach their final user. This is often the case, for example, when a product is sent to the distribution branch of a manufacturer; or it is offered for sale online or through other means of distance selling and is transferred to fulfilment service providers for delivery, reaching its final user days or months after placement on the market. For example, a laptop may stay on the shelf of an electronics shop for some time before being reaching its user.

In the period between placement on the market and transaction to the intended final user, known exploitable vulnerabilities affecting that product may be discovered. However, the obligation to deliver, on the basis of the risk assessment, products without known exploitable vulnerabilities applies at the moment of placement on the market (Article 13(1)). As the product has already been placed on the market, manufacturers are therefore not expected to fix newly discovered vulnerabilities while their products have not yet reached their user.

Nonetheless, as the CRA also establishes vulnerability handling requirements that apply during a product's support period, manufacturers shall, in relation to the risks posed to products with digital elements, address and remediate vulnerabilities without delay, in accordance with Annex I, Part II, point (2). For example, given the risks posed by the newly discovered exploitable vulnerabilities, the laptop manufacturer establishes that a security update is necessary to address those vulnerabilities. The manufacturer may be required to provide a security update for the laptop, as soon as it is put into operation by its user.

4.2.4 How does the secure-by-default requirement work?

> *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* (Annex I, Part I, point 2(b)).

Manufacturers are required to place products with digital elements on the market with a secure by default configuration, in light of that product's intended purpose and reasonably foreseeable use, and on the basis of the manufacturer's cybersecurity risk assessment.

Where manufacturers place on the market a component for integration into another product with digital elements, they do not retain control on how the integrating manufacturer adjusts the component's configuration. The obligation to ensure a secure-by-default configuration, therefore, only applies to the component when it is placed on the market separately, and not to how it is later configured or deployed by integrating manufacturers.

For example, the manufacturer of a cryptographic library may be required, on the basis of its risk assessment, to place that library on the market with insecure or deprecated algorithms disabled by default, or certificate validation enabled by default. The integrating manufacturer may decide to change some of those settings when developing its own product with digital elements. The manufacturer of the cryptographic library is only responsible for the configuration that the library is delivered with, and not for subsequent modifications that its integrator makes.

Similarly, the manufacturer of a microcontroller with a built-in network stack may be required, on the basis of its risk assessment, to place the microcontroller on the market with the network interfaces disabled by default. The integrating manufacturer may then decide to enable them to meet its own product's intended purpose. The manufacturer of the microcontroller is only responsible for the configuration that the microcontroller is delivered with, and not for subsequent modifications that its integrator makes.

For further information on exceptions to the secure-by-default configuration, see entry *4.2.5 When is a product "tailor-made"? What documentation is required in these cases?*

Finally, it is possible that this essential requirement is not applicable to some products with digital elements. Entry *4.1.3 Does a manufacturer need to implement all the essential requirements?* provides further guidance on this.

4.2.5 When is a product "tailor-made"? What documentation is required in these cases?

Manufacturers should make their products with digital elements available on the market with a secure by default configuration and provide security updates to users free of charge. 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 (Recital 64).

The CRA establishes that manufacturers may deviate from two essential requirements (namely, secure by default configuration in point (2.b) of Annex I, Part I and providing security updates to users free of charge in point (8) of Annex I, Part II) 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, as stated in the aforementioned points of Annex I, Part I.

This could be the case, for example, for custom-developed hardware or software designed to meet the needs of a specific business user, or products that are developed for integration into a specific customer's highly controlled environments (e.g. closed networks or air-gapped environments) and are subject to specific contractual terms.

A product is not tailor-made, on the other hand, when it undergoes minor customisations before being sold to a customer, without specific sets of contractual terms or arrangements. This is the case, for example, for a customer relationship management (CRM) platform sold to multiple businesses, even if the manufacturer enables some minor customisations; or platforms that use plugins or APIs to be customised, but are fundamentally the same product for every customer.

In accordance with Article 31, the manufacturer is expected to include in its technical documentation all relevant data or details to show that its product complies with the relevant essential cybersecurity requirements, including appropriate evidence to demonstrate that the product is tailor-made.

4.3 Vulnerability handling obligations (Annex I, Part II)

4.3.1 Are manufacturers required to patch all vulnerabilities that are discovered during the support period?

> *Manufacturers of products with digital elements shall […] in relation to the risks posed to products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates* (Annex I, Part II, point 2).

The CRA does not require manufacturers to provide a patch for all vulnerabilities that are discovered during a product's support period. When discovering a vulnerability, manufacturers are expected to determine its relevance for their product, and assess the resulting risk, in the framework of the manufacturer's risk assessment. On the basis of the risk that the vulnerability poses, manufacturers need to ensure that remedies are put in place without delay. The CRA does not therefore prescribe that manufacturers must provide a patch for all vulnerabilities that are discovered during a product's support period.

Depending on the risk, remedies may take different forms, including but not limited to immediate patches, advisories on workarounds to be later complemented by a software updates, updates to user manuals, configuration guidance to disable the affected features.

For example, a manufacturer of a smart home hub finds a vulnerability in its product which allows remote attackers to execute arbitrary code on the hub; the manufacturer's risk assessment shows that there is a high risk of compromise, as the attacker could control other connected devices. The manufacturer may be expected, for example, to provide an immediate patch and appropriate guidance to its users.

On the other hand, a manufacturer of a Wi-Fi router finds a buffer overflow vulnerability in one of the software libraries contained in the router's firmware; the manufacturer's risk assessment, however, shows that the vulnerability cannot be exploited, as the library functions are never called in the firmware. The manufacturer may be expected, for example, to document the vulnerability, but may decide not to fix it with a dedicated update. The manufacturer may also be expected, for example, to remove the unused library in its next regular firmware release.

Finally, a manufacturer of an office laser printer discovers that the printer's motherboard has a debugging interface that remains enabled. While the vulnerability could theoretically be exploited to bypass authentication and inject malicious code, exploiting the vulnerability requires physical access to the printer, breaking its tamper-evident seal, disassembling internal components and soldering to the motherboard. The manufacturer's risk assessment shows that the vulnerability presents a very low risk and has no exploitability in its operational environment. The manufacturer may be expected, for example, to document the vulnerability, update its technical documentation and provide appropriate recommendations to its users.

4.3.2 Does the manufacturer need to address and remediate vulnerabilities for all versions of a software product?

Where a manufacturer has placed subsequent substantially modified versions of a software product on the market, that manufacturer may ensure compliance with the essential cybersecurity requirement set out in Part II, point (2), of Annex I only for the version that it has last placed on the market, provided that the users of the versions that were previously placed on the market have access to the version last placed on the market free of charge and do not incur additional costs to adjust the hardware and software environment in which they use the original version of that product (Article 13.10).

Recital 40 explains in detail the provision of Article 13.10, clarifying that manufacturers are not required to address and remediate vulnerabilities for all versions of a software product, if certain criteria are met.

Specifically, "*taking into account the iterative nature of software development, manufacturers that have placed subsequent versions of a software product on the*

market as a result of a subsequent substantial modification of that product should be able to provide security updates for the support period only for the version of the software product that they have last placed on the market. They should be able to do so only if the users of the relevant previous product versions have access to the product version last placed on the market free of charge and do not incur additional costs to adjust the hardware or software environment in which they operate the product. This could, for instance, be the case where a desktop operating system upgrade does not require new hardware, such as a faster central processing unit or more memory. Nonetheless, the manufacturer should continue to comply, for the support period, with other vulnerability-handling requirements, such as having a policy on coordinated vulnerability disclosure or measures in place to facilitate the sharing of information about potential vulnerabilities for all subsequent substantially modified versions of the software product placed on the market. Manufacturers should be able to provide minor security or functionality updates that do not constitute a substantial modification only for the latest version or sub-version of a software product that has not been substantially modified. At the same time, where a hardware product, such as a smartphone, is not compatible with the latest version of the operating system it was originally delivered with, the manufacturer should continue to provide security updates at least for the latest compatible version of the operating system for the support period" (Recital 40).

4.3.3 Is the manufacturer responsible for the installation of security updates by the product's users?

One of the most important measures for users to take in order to protect their products with digital elements from cyberattacks is to install the latest available security updates as soon as possible. Manufacturers should therefore design their products and put in place processes to ensure that products with digital elements include functions that enable the notification, distribution, download and installation of security updates automatically, in particular in the case of consumer products. They should also provide the possibility to approve the download and installation of the security updates as a final step. Users should retain the ability to deactivate automatic updates, with a clear and easy-to-use mechanism, supported by clear instructions on how users can opt out. The requirements relating to automatic updates as set out in an annex to this Regulation are not applicable to products with digital elements primarily intended to be integrated as components into other products. They also do not apply to products with digital elements for which users would not reasonably expect automatic updates, including products with digital elements intended to be used in professional ICT networks, and especially in critical and industrial environments where an automatic update could cause interference with operations. Irrespective of whether a product with digital elements is designed to

receive automatic updates or not, its manufacturer should inform users about vulnerabilities and make security updates available without delay (Recital 56)

Products with digital elements shall be made available on the market only where: (a) they meet the essential cybersecurity requirements set out in Part I of Annex I, provided that they are properly installed, maintained, used for their intended purpose or under conditions which can reasonably be foreseen, and, where applicable, the necessary security updates have been installed; and (b) the processes put in place by the manufacturer comply with the essential cybersecurity requirements set out in Part II of Annex I (Article 6)

On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall: (c) ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic security updates that are installed within an appropriate timeframe enabled as a default setting, with a clear and easy-to-use opt-out mechanism, through the notification of available updates to users, and the option to temporarily postpone them (Annex I, Part I, point (2)(c)).

Manufacturers of products with digital elements shall: (7) provide for mechanisms to securely distribute updates for products with digital elements to ensure that vulnerabilities are fixed or mitigated in a timely manner and, where applicable for security updates, in an automatic manner (Annex I, Part II, point (7)).

Manufacturers of products with digital elements shall: (8) ensure that, where security updates are available to address identified security issues, they are disseminated without delay and, unless otherwise agreed between a manufacturer and a business user in relation to a tailor-made product with digital elements, free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken. (Annex I, Part II, point (8)).

The CRA establishes a series of mechanisms that require manufacturers to ensure that security updates are disseminated without delay, that such updates are installed automatically where possible, and that users of products with digital elements are kept duly informed. The CRA also recognises that automatic updates are not always applicable, and users should also have the possibility to postpone the installation of such updates.

The manufacturer is not responsible under the CRA if the user does not install security updates, e.g. where updates are not installed either because automatic updates are not applicable or because the user opts out.

4.3.4 Does the manufacturer need to recall the product if it cannot fix a vulnerability?

From the placing on the market and for the support period, manufacturers who know or have reason to believe that the product with digital elements or the processes put in place by the manufacturer are not in conformity with the essential cybersecurity requirements set out in Annex I shall immediately take the corrective measures necessary to bring that product with digital elements or the manufacturer's processes into conformity, or to withdraw or recall the product, as appropriate (Article 13(21)).

As explained in *4.3.1 Are manufacturers required to patch all vulnerabilities that are discovered during the support period?*, the manufacturer is required, in relation to the risks posed, to address and remediate vulnerabilities during the support period. Appropriate remedies can take different forms, including mitigation measures.

In some circumstances, however, it is possible that a vulnerability that presents a very significant risk of compromise, particularly in a hardware product with digital elements, cannot be addressed and remediated adequately and the product cannot be brought back into conformity. In such cases, which are likely to be exceptional cases, the manufacturer may be required to withdraw or recall the product, as appropriate.

It is likely that, in such circumstances, the relevant market surveillance authorities are involved and that the relevant procedures laid down in Articles 54-58 of the CRA are activated.

4.3.5 How should manufacturers ensure a separation between security and functionality updates, particularly where updates serve both purposes?

Manufacturers of products with digital elements shall: (2) in relation to the risks posed to products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates; where technically feasible, new security updates shall be provided separately from functionality updates (Annex I, Part II, point (2)).

To improve the transparency of vulnerability handling processes and to ensure that users are not required to install new functionality updates for the sole purpose of receiving the latest security updates, manufacturers should ensure, where technically feasible, that new security updates are provided separately from functionality updates (Recital 57).

The CRA establishes that manufacturers should, where technically feasible, provide new security updates separately from functionality updates, in order to ensure that updates can be delivered in a prompt manner and that users are not required to install functionality updates to be able to receive the latest security updates.

Manufacturers that release a security update to address a vulnerability are not to bundle that update with other functionality updates. For example, a smart home device has a vulnerability in the SSL certificate validation process that enables an attacker to perform a man-in-the-middle attack. To fix the vulnerability, it is sufficient for the manufacturer to update the SSL certificate validation routine. The manufacturer should deliver that update separately, without bundling the security fix with other functionality-related updates.

Nonetheless, where a functionality update is necessary to deliver a security update, the essential requirements do not prevent the manufacturer to deliver an update that combines both security and functionality modifications. For example, a PDF reader has a vulnerability that is contained in an outdated file format parser and which triggers buffer overflows. The fix requires replacing the file format parser with a new, safer parser that supports a slightly different behaviour (e.g. stricter format checking), and which may lead to some functionality changes, because some files that worked before may now be rejected. As it would not be technically feasible, the manufacturer is not required to ensure a separation between these types of software modifications.

Similarly, in certain situations, the functionality update can itself correspond to the security update. For example, a product with digital elements accesses the same feature via different interfaces (e.g. web interface, mobile app interface, command-line interface, API endpoint). If one of those interfaces contains a vulnerability, the manufacturer may determine that it is necessary to disable that vulnerable interface – thereby delivering a functionality update that is also a security update.

4.3.6 How should vulnerabilities in integrated components be addressed and remediated?

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 (Recital 34).

Manufacturers need to comply with the vulnerability handling obligations for the duration of the support period, for their products in their entirety, including by handling vulnerabilities affecting their products that are contained in integrated components. See also *4.3.1 Are manufacturers required to patch all vulnerabilities that are discovered during the support period?*

Where the manufacturer of a product has integrated a component that has been placed on the market after CRA applies (i.e. the component is itself a product under the CRA), that manufacturer is able to rely on the actions that the component manufacturer is required to undertake to comply with its own vulnerability handling obligations. For example, the component manufacturer may be required to develop a security update to fix a vulnerability in the component. The integrating manufacturer is still required to fulfil its vulnerability handling obligations for its product, for example by keeping users informed, providing mitigating measures, updating documentation; but its vulnerability handling obligations are facilitated by the corresponding obligations of the component manufacturer.

Where the manufacturer has integrated a component that has not been placed on the market (or that has been placed on the market before the CRA applies), the person or entity that has developed the component is not subject to the CRA vulnerability handling obligations. The integrating manufacturer is nonetheless required to ensure that its product complies in its entirety with the vulnerability handling requirements. Where the person or entity that has developed the component is not supporting the manufacturer in addressing and remediating vulnerabilities, the integrating manufacturer is expected to address the vulnerability via other means, for example by disabling compromised functions; switching out the affected component; developing by itself a patch (for example, where the component is open source component).

In accordance with Article 13(6), where the integrating manufacturer develops a patch for a component, it is required to share it with the person or entity maintaining the component.

4.3.7 How does the end of the support period in an integrated component impact a product's compliance with the CRA?

> *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 [...]* (Article 13.8)

Manufacturers need to comply with the vulnerability handling obligations for the duration of the support period, for their products in their entirety, including all integrated components, but are able to rely on the vulnerability handling obligations to which component manufacturers are also subject, as discussed in entry *4.3.6 How should vulnerabilities in integrated components be addressed and remediated?*

The support period of integrated components is a consideration that manufacturers may take into account when determining their product's support period, to ensure that they

are able to leverage the support period of key components to address and remediate the product's vulnerabilities. See also section *4.5 Support period*.

Nonetheless, it can occur that a product with an active support period contains a vulnerability in an integrated component that is no longer covered by that component's support period, and that vulnerability cannot be addressed and remediated adequately via various forms of mitigation measures (see also entry *4.3.1 Are manufacturers required to patch all vulnerabilities that are discovered during the support period?*). In that case, the manufacturer of the product is required to remediate the vulnerability via other means, for example by switching out the integrated component or developing a patch autonomously.

4.4 Due diligence requirements for integrating components

4.4.1 What does the CRA prescribe when integrating components?

When placing a product with digital elements on the market, manufacturers shall ensure that it has been designed, developed and produced in accordance with the essential cybersecurity requirements set out in Part I of Annex I (Article 13(1))

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 (Article 13(5))

When 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 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 [...] (Recital 34)

Immediately after the transitional period for the application of this Regulation, a manufacturer of a product with digital elements that integrates one or several components sourced from third parties which are also subject to this Regulation may not be able to verify, as part of its due diligence obligation, that the manufacturers of those components have demonstrated conformity with this Regulation by checking, for instance, if the components already bear the CE marking. This may be the case where the components have been integrated before this Regulation becomes applicable to the manufacturers of those components. In such a case, a manufacturer integrating such components should exercise due diligence through other means (Recital 35)

In order to ensure that their product with digital elements meets the essential requirements of the CRA, manufacturers are to exercise due diligence when they integrate third-party components in their products.

Manufacturers can integrate different types of components, including those that do not bear the CE marking (e.g. free and open-source components that do not fall in the scope of the CRA, components placed on the market before the CRA applies, or components that have not been placed on the market), but they must ensure that such components do not compromise the cybersecurity of their products with digital elements.

When integrating components that bear the CE marking, manufacturers are able to rely on the component's EU declaration of conformity and accompanying documentation to support their own compliance with the CRA.

The appropriate level of due diligence depends on the nature and level of cybersecurity risk of a given component – see also entry on *4.4.2 What is the appropriate level of due diligence?*

4.4.2 What is the appropriate level of due diligence?

The appropriate level of due diligence depends on the nature and level of cybersecurity risk of a given component and is aimed at ensuring that the components that are integrated do not compromise the cybersecurity of the manufacturer's product with digital elements. The risk assessment of the product with digital elements also informs the appropriate level of due diligence. Where a component or a product is associated with more risks, the actions that a manufacturer should put in place while exercising due diligence should be more extensive than for a component or product associated with fewer risks. In line with Recital 34, examples of one or more actions that manufacturers may undertake include:

- 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 in the European vulnerability database established pursuant to Article 12(2) of Directive (EU) 2022/2555 or other publicly accessible vulnerability databases the vulnerabilities applicable to a component and designing, developing and manufacturing the product with digital elements integrating the component in such a way that these vulnerabilities do not compromise the cybersecurity of the product with digital elements;
- carrying out additional security tests, such as fuzz testing, penetration testing, firmware analysis, side-channel analysis, red-team exercises, network traffic analysis, sensor spoofing.

Additional examples of actions that manufacturers may undertake include:

- performing software composition analysis on components;
- sandboxing or isolating highly-critical components;
- when available, reviewing the SBOM of that component;
- checking the support period of the component;
- verifying that the intended purpose of the component fits the integrating manufacturer's use;
- assessing the security posture of the component's manufacturer.

4.4.3 In order to exercise due diligence, should a manufacturer only integrate components that bear the CE marking?

In line with Article 13(5), manufacturers can integrate various types of components, including components that have not been placed on the market or that have been placed on the market before the CRA applies, provided that it exercises due diligence to ensure that the component does not compromise the cybersecurity of its own product with digital elements.

The manufacturer does not need to bring such components into compliance with the essential requirements set out in Annex I, part I, before integrating them.[8]

Nonetheless, the manufacturer needs to ensure that its own products with digital elements are secure and meet the CRA essential requirements, and due diligence is a key obligation to meet those requirements. The manufacturer is also required to comply with the vulnerability handling obligations of Annex I, Part II, for the duration of the support period, for their products in their entirety.

[8] Manufacturers of such components are required to ensure they are compliant with the CRA, if they place them on the market.

Integration of components that bear the CE marking may simplify certain obligations (e.g. see entry *4.3.6 How should vulnerabilities in integrated components be addressed and remediated?*) but is not required by the CRA.

4.4.4 How should manufacturers exercise due diligence with regards to open-source components that are not subject to the CRA?

Manufacturers are allowed to integrate open-source components that are not in scope of the CRA (i.e. because they are not made available on the market in the course of a commercial activity), as well as open-source components that are published by an open-source software steward.

As explained in *4.4.2 What is the appropriate level of due diligence?*, the appropriate level of due diligence is dependent on the nature and level of cybersecurity risk of a given open-source component.

The Commission is empowered to establish voluntary security attestations programmes that can be used to assess the conformity of free and open-source components with the CRA. Where available, such attestation programmes would facilitate manufacturers' due diligence obligation.

4.5 Support period

4.5.1 Which criteria should the manufacturer take into account when determining a product's support period?

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 (Article 13(8), second subparagraph).

Manufacturers are required to determine the support period so that it reflects the length of time during which it is expected to be in use, taking into account, in particular:

- reasonable user expectations;
- the nature of the product, including its intended purpose;
- other Union law determining the lifetime of products with digital elements.

Other relevant factors that manufacturers may take into account include:

- the support period of similar products placed on the market by other manufactures;
- the availability of the operating environment;
- the support period of third-party integrated components providing core functions;
- relevant guidance provided by the CRA ADCO.

All these factors should be taken into account in a manner that ensures proportionality in the determination of the support period.

Therefore, manufacturers are not expected to simply set support periods that correspond to the expected use time (unless the expected use time is less than five years, as discussed in entry *4.5.2 Is there a minimum support period?)*.

In accordance with Article 13(8), a manufacturer should include in its technical documentation the information that was taken into account to determine the support period of a product with digital elements.

4.5.2 Is there a minimum support period?

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 (Article 13(8), third subparagraph).

The support period for which the manufacturer ensures the effective handling of vulnerabilities should be no less than five years, unless the lifetime of the product with digital elements is less than five years, in which case the manufacturer should ensure the vulnerability handling for that lifetime. Where the time the product with digital elements is reasonably expected to be in use is longer than five years, as is often the case for hardware components such as motherboards or microprocessors, network devices such as routers, modems or switches, as well as software, such as operating systems or video-editing tools, manufacturers should accordingly ensure longer support periods. In particular, products with digital elements intended for use in industrial settings, such as industrial control systems, are often in use for significantly longer periods of time. A manufacturer should be able to define a support period of less than five years only where

this is justified by the nature of the product with digital elements concerned and where that product is expected to be in use for less than five years, in which case the support period should correspond to the expected use time. For instance, the lifetime of a contact tracing application intended for use during a pandemic could be limited to the duration of the pandemic. Moreover, some software applications can by nature only be made available on the basis of a subscription model, in particular where the application becomes unavailable to the user and is consequently not in use anymore once the subscription expires (Recital 60)

The support period needs to be set to at least five years, but that is not sufficient where products with digital elements are reasonably expected to be in use for longer than five years. In such circumstances, manufacturers should consider all relevant factors (see entry *4.5.1 Which criteria should the manufacturer take into account when determining a product's support period?*) which may result in a need to provide for a support period longer than five years.

A support period of less than five years is only justified in situations where the lifetime of the product with digital elements is less than five years. In these cases, the support period shall correspond to the expected use time, without further consideration for the other criteria listed in Article 13(8). This is the case for products that fulfil a very specific purpose (e.g. a contact tracing app to be used during a pandemic), but also for some software applications that can, by nature, only be made available on the basis of a subscription model, particularly where the application becomes unavailable to the user once the subscription expires. For example, some enterprise antivirus software only works for users with an active subscription, as users rely on the availability of up-to-date antivirus definitions, and is no longer accessible when that subscription expires. Similarly, some free and open-source software that is placed on the market can be monetised by its manufacturer only through the sale of paid support services offered on a subscription basis. Therefore, due to its nature of being free and open-source, that software may remain in use after its user stops paying for the support services; in such circumstance, the manufacturer is required to ensure a support period that is equal to the duration of the active subscription.

4.5.3 Can a manufacturer continue to sell products without a support period?

Manufacturers need to set the support period for all products with digital elements that have been placed on the market after 11 December 2027. Those products can continue to be made available on the market after their support period expires. However, for units of that product that are newly placed on the market, manufacturers are required to set the support period.

For example, a manufacturer produces 10 000 identical units of the same hardware product model or series and places them on the market in January 2028, with a support period of five years (i.e. until January 2033). A distributor manages to sell only a part of those units before the end of the support period. The distributor can continue to make those units available even after January 2033.

On 1 January 2030, the same manufacturer produces an additional 5 000 identical units of that same hardware product model or series and places them on the market. The manufacturer is required to set a support period for those units, in accordance with Article 13(8) of the CRA.

4.6 Other manufacturer's obligations

4.6.1 Can a third-country manufacturer directly place products on the Union market?

1. Notwithstanding any obligations set out in applicable Union harmonisation legislation, a product subject to legislation referred to in paragraph 5 may be placed on the market only if there is an economic operator established in the Union who is responsible for the tasks set out in paragraph 3 in respect of that product.

2. For the purposes of this Article, the economic operator referred to in paragraph 1 means any of the following:

(a) a manufacturer established in the Union;

(b) an importer, where the manufacturer is not established in the Union;

(c) an authorised representative who has a written mandate from the manufacturer designating the authorised representative to perform the tasks set out in paragraph 3 on the manufacturer's behalf;

*(d) a fulfilment service provider established in the Union with respect to the products it handles, where no other economic operator as mentioned in points (a), (b) and (c) is established in the Union (*Article 4(1) and (2) of Regulation (EU) 2019/1020)

A product with digital elements can be placed on the Union market if there is an economic operator established in the Union that is responsible *inter alia* to verify that the EU declaration of conformity and the technical documentation have been drawn up and to cooperate with market surveillance authorities.

A manufacturer who is not established in the Union, therefore, is required to have an importer, an authorised representative or a fulfilment service provider to perform those tasks.

5 Reporting obligations of manufacturers

5.1 How can a manufacturer become aware of an actively exploited vulnerability or a severe incident?

The CRA does not specify how a manufacturer is to become aware of an actively exploited vulnerability or a severe incident, but rather imposes the obligation to notify in accordance with Articles 14 once it does.

The paragraphs below provide some examples on how a manufacturer may become aware of such vulnerabilities or incidents, via a variety of activities and channels. It should be noted that this does not imply that the manufacturer is required to carry out such activities or monitor such channels to comply with the reporting obligations.[9]

For example, a manufacturer may become aware because a customer or a partner organisation inform it of unusual activity or compromise, providing the manufacturer with reliable evidence that an actively exploited vulnerability is contained in its product (or the manufacturer gathers reliable evidence confirming its existence).

A manufacturer may also become aware via threat intelligence reports, e.g. security researchers or cybersecurity firms publish reports detailing a zero-day vulnerability (i.e. a vulnerability for which a patch or a security update is not yet available) in the manufacturer's product being used in targeted attacks. Governmental cybersecurity agencies may also notify the manufacturer, having detected exploitation of a vulnerability through their monitoring systems. Ethical hackers may also report a vulnerability that is already being exploited in the wild.

Furthermore, the manufacturer may also become aware via internal monitoring, scanning activities or telemetry. For example, the manufacturer's telemetry system or honeypot (i.e. a security mechanism used to lure cybercriminals away from legitimate targets) indicates exploitation of a previously unknown vulnerability in the manufacturer's product, or the manufacturer's security team monitors dark web forums and finds evidence that hackers have successfully exploited a vulnerability in the manufacturer's product.

[9] Nonetheless, Annex I, Part II does require the manufacturer to have, inter alia, a single point of contact where vulnerabilities can be reported, to put in place and enforce a coordinated vulnerability disclosure policy and take measures to facilitate the sharing of information about potential vulnerabilities.

5.2 Does a manufacturer need to report zero-day vulnerabilities?

'actively exploited vulnerability' means a vulnerability for which there is reliable evidence that a malicious actor has exploited it in a system without permission of the system owner (Article 3(42))

Actively exploited vulnerabilities concern instances where a manufacturer establishes that a security breach affecting its users or any other natural or legal persons has resulted from a malicious actor making use of a flaw in one of the products with digital elements made available on the market by the manufacturer. Examples of such vulnerabilities could be weaknesses in a product's identification and authentication functions. Vulnerabilities that are discovered with no malicious intent for purposes of good faith testing, investigation, correction or disclosure to promote the security or safety of the system owner and its users should not be subject to mandatory notification (Recital 68)

Vulnerabilities for which a patch or a security update is not yet available (so-called 'zero-day vulnerabilities') are subject to reporting in accordance with Article 14, when the manufacturer has reliable evidence that a malicious actor has exploited that vulnerability.

For example, a zero-day vulnerability discovered by ethical hackers, for which there is no evidence of previous malicious exploitation, and which is disclosed to the product's manufacturer as part of its bug-bounty programme (see Recital 76) is not an actively exploited vulnerability subject to mandatory reporting. Similarly, a zero-day vulnerability discovered by a cybersecurity assessment laboratory performing tests on behalf of the manufacturer, and for which there is no evidence of previous malicious exploitation, is not an actively exploited vulnerability subject to mandatory reporting. Manufacturers may still notify those vulnerabilities on a voluntary basis, in accordance with Article 15.

5.3 Does a manufacturer need to report actively exploited vulnerabilities or severe incidents for products placed on the market before the CRA applies?

By way of derogation from paragraph 2 of this Article, the obligations laid down in Article 14 shall apply to all products with digital elements that fall within the scope of this Regulation that have been placed on the market before 11 December 2027 (Article 69(3)).

Reporting obligations start applying as of 11 September 2026. Manufacturers are required to comply with Article 14, and particularly with the obligation to notify actively exploited vulnerabilities and severe incidents having an impact on the security of the product for all products with digital elements falling within the scope of the CRA, including products that have been placed on the market before 11 December 2027.

If the product has been placed on the market before 11 December 2027, manufacturers may not be able to investigate such vulnerabilities, for example because tooling to scan or run old software versions may no longer exist, build environments for old code may be impossible to recreate, dependencies may be unavailable or incompatible with modern systems, staff with knowledge of old codebases may have left. For such products, manufacturers are required to notify the vulnerability or incident but are not required by the CRA to comply with other obligations, e.g. in relation to vulnerability handling.

Furthermore, the obligation to notify applies upon becoming aware following the entry into application of the reporting requirements (see also entry *5.1 How can a manufacturer become aware of an actively exploited vulnerability or a severe incident?*).

Nonetheless, Article 14(8) requires the manufacturer to inform the impacted users of the product with digital elements, and where appropriate all users, of those vulnerabilities or incidents. Where the manufacturer decides not to inform the users of the product with digital elements in a timely manner, the CSIRTs that receive the notification may provide such information to the users when considered to be proportionate and necessary for preventing or mitigating the impact of that vulnerability or incident.

5.4 If an actively exploited vulnerability is contained in a third-party component, are all manufacturers integrating that component required to notify it?

'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 (Article 3(10))

A manufacturer shall notify any actively exploited vulnerability contained in the product with digital elements that it becomes aware of (Article 14(1))

Manufacturers should notify actively exploited vulnerabilities to ensure that the CSIRTs designated as coordinators, and ENISA, have an adequate overview of such vulnerabilities and are provided with the information necessary to fulfil their tasks as set out in Directive (EU) 2022/2555 and raise the overall level of cybersecurity of essential and important entities as referred to in Article 3 of that Directive, as well as to ensure the effective functioning of market surveillance authorities. As most products with digital elements are marketed across the entire internal market, any exploited vulnerability in a product with digital elements should be considered to be a threat to the functioning of the internal market (Recital 66)

Manufacturers are required to notify any actively exploited vulnerability contained in their product with digital elements. Where the product with digital elements contains an

actively exploited vulnerability originating from an integrated component, the manufacturer of the product with digital elements is required to notify that vulnerability. The manufacturer of the integrated component is also required to notify it, if that component has been placed on the market.

If the manufacturer of a product with digital elements is aware that an integrated component contains a vulnerability, but that vulnerability cannot be exploited in its product with digital elements, that vulnerability is not actively exploited, and therefore it is not subject to mandatory reporting. Manufacturers can still notify that vulnerability on a voluntary basis, in accordance with Article 15, and are required to report the vulnerability to the person or entity manufacturing or maintaining the component, in accordance with Article 13(6).

This enables the CSIRTs receiving the notification and ENISA to have an overview of the security landscape in the internal market and to assess the level of criticality and market penetration of actively exploited vulnerabilities.

6 Conformity assessment

The conformity assessment is a legal procedure to be implemented by the manufacturer to demonstrate that the product with digital elements is compliant with the essential requirements of the CRA.

The CRA provides the following options:

- Module A, or conformity based on internal control, set out in part I of Annex VIII.
- Module B+C, or EU-type examination, set out in Parts II and III of Annex VIII.
- Module H, or conformity based on full quality assurance, set out in Part IV of Annex VIII.

The three modules above are indicated in increasing order of complexity, cost but also external support to manufacturers.

6.1 What is module A? How does it work? What conformity assessment activities are expected for self-assessment?

Module A, set out in part I of Annex VIII, is a conformity assessment procedure in which the manufacturer verifies that the product with digital elements complies with the essential requirements of the CRA and declares compliance on its sole responsibility.

No notified bodies participate in this procedure.

The following categories of products are allowed to use module A:

- All products with digital elements that do not have the core functionality of a category of important or critical products ('default category').
- Important products with digital elements of class I, if a harmonised standard has been applied in accordance with Article 32(2);
- Important products with digital elements of class I or II, if they are free and open-source software provided that the technical documentation is made available to the public, in accordance with Article 32(5).

The manufacturer has to perform the following activities:

- Implement the necessary cybersecurity mitigation measures in the product following the risk assessment described in section *4.1 Risk-based approach and risk-assessment*.
- Verify (via testing or other mechanism) that the product complies to the relevant essential requirements of the CRA. When applicable, see also section *6.5 Which evaluation methodology should a manufacturer apply?*
- Draw up the technical documentation. See also section *6.6 What is the technical documentation?*

- Once the manufacturer is in a position to demonstrate that the product with digital elements is compliant with the CRA essential requirements, affix the CE marking (see section *6.7 What is the CE marking?*), draw up and sign a declaration of conformity (see section *6.8 What is the declaration of conformity?*).
- Ensure that the production of the different units of the product with digital elements does not alter the compliance with the CRA essential requirements.

6.2 What is module B+C? How does it work?

Module B+C, set out in Parts II and III of Annex VIII, is a conformity assessment procedure in which the manufacturer verifies that the product with digital elements complies with the essential requirements of the CRA, a notified body examines the design and development of the product, and the manufacturer declares compliance.

The manufacturer can undertake a conformity assessment procedure based on module B+C for all categories of products covered by the CRA. Module B+C or H are mandatory in the following cases[10]:

- Important products with digital elements of class I if a harmonised standard has not been applied, in accordance with Article 32(2).
- Important products of class II.
- Critical products (unless the use of a European cybersecurity certification scheme is made mandatory in the future in accordance with Article 8(1).

Only one notified body participates in this procedure and examines the whole product and all relevant essential requirements in the terms described below.

The manufacturer and the notified body have to perform the following activities:

- The manufacturer implements the necessary cybersecurity mitigation measures in the product following the risk assessment described in section *4.1 Risk-based approach and risk-assessment*.
- The manufacturer tests the product in order to verify that it complies with the relevant essential requirements of the CRA. See for further information section *6.5 Which evaluation methodology should a manufacturer apply?*
- The manufacturer draws up the technical documentation. See for further information section *6.6 What is the technical documentation?*
- The notified body assesses the design of the product, based on its technical documentation, and one specimen or sample. The notified body does not only

[10] In accordance with Article 32(5), manufacturers retain the possibility to use module A even in the case of an important product with digital elements of class I or II if their product qualifies as free and open-source software and the technical documentation is made available to the public.

carry out a documentation-based assessment, but it additionally performs the necessary tests, either itself or via an external laboratory. The manufacturer might need to be involved in those tests. Once the notified body concludes that the product is compliant with the CRA, it issues an EU-type certificate, which is valid for a certain period of time, as defined by the notified body.

- Once the manufacturer obtains the EU-type certificate, it affixes the CE marking (see section 6.7 What is the CE marking?) together with the NANDO number of the notified body, draw up and sign a declaration of conformity (see *section 6.8 What is the declaration of conformity?*).
- The manufacturer ensures that the production of the different units of the product does not alter the compliance with the CRA essential requirements, as laid down in point 2 of module C. The production phase is not assessed by the notified body. In other words, the manufacturer cannot justify that a product whose design is compliant with the CRA is not, in the practice, compliant because of a defect in the production process.

Substantial modifications of the product require a new assessment by the same or a different notified body, that might lead to a potential revision of the issued EU-type certificate. Other modifications that do not affect the compliance with the CRA requirements are not subject to reassessment by the notified body. Additionally, in accordance with point 8 of module B, the notified body must carry out periodic audits to ensure that the vulnerability handing processes are properly implemented.

Information about EU-type certificates and their revisions has to be shared with other notified bodies and with the notifying authorities, according to point 9 of module B.

6.3 What is module H? How does it work?

Module H, set out in Part IV of Annex VIII, is a conformity assessment procedure in which the manufacturer implements a full quality control system that ensures that the products subject to this system comply with the essential requirements of the CRA in both the design and the production phases. A notified body assesses the overall performance of the quality control system, including periodical tests and checks. The manufacturer declares compliance with the CRA requirements before placing the products on the market.

Only one notified body participates in this procedure and examines the whole quality control system in the terms described below.

This module might be particularly considered by manufacturers that place numerous product types on the market or products subject to frequent updates, since it streamlines

the relevant conformity assessment procedures for each new or substantially modified product.

The manufacturer and the notified body have to perform the following activities:

- The manufacturer implements a full quality control system that covers a certain catalogue of products and all the relevant manufacturing phases, from design to production. The system can be based on international standards (for example, ISO 9000 series covering the specificities of the CRA). The fact that the manufacturer is accredited against the standard ISO 9000 does not automatically entitle it to perform conformity assessment activities under module H, since the involvement of a CRA notified body is needed.
- The notified body assesses the quality control system as a whole, including, among others, the technical design of the covered products, the standards or specifications to be applied (in particular, how the compliance with the essential requirements of the CRA is ensured), the tests to be performed, and the monitoring of the overall system. The notified body covers the whole manufacturing process.
- The manufacturer, based on the quality control system, implements the necessary cybersecurity mitigation measures in the product following the risk assessment described in section *4.1 What does the CRA require of the manufacturer's cybersecurity risk assessment?*.
- The manufacturer, based on the quality control system, tests the product in order to verify that it complies to the relevant essential requirements of the CRA. See for further information section *6.5 Which evaluation methodology should a manufacturer apply?*
- The manufacturer, based on the quality control system, draws up the technical documentation. See for further information section *6.6 What is the technical documentation?*
- The manufacturer affixes the CE marking (see section *6.7 What is the CE marking?*) together with the NANDO number of the notified body, draws up and signs a declaration of conformity (see section *6.8 What is the declaration of conformity?*).
- The manufacturer, based on the quality control system, ensures that the production of the different units of the product does not alter the compliance with the CRA essential requirements.

The manufacturer can extend the scope of the described quality system to new or substantially modified products. The quality system must be updated in order to properly document the new scope, and potential new standards might need to be applied or tests might need to be performed. Nevertheless, this extension is subject to a new assessment by the same notified body that performed the original assessment. In any case, and as

indicated above, module H provides a more versatile and flexible framework compared to module B+C. Hence, the inclusion of new products constitutes a more streamlined process, since the notified body will only have to assess the potential new standards or tests applicable to the new products.

6.4 Are manufacturers required to ensure the conformity of "existing" product types?

The CRA is applicable to products placed as individual units on the market as of its date of applicability. In other words, legacy types or models are not exempted from the application of the CRA if, after the aforementioned date, new units are placed on the market. The CRA provides a transition period between its entry into force (10 December 2024) and its date of application (11 December 2027 for the majority of the obligations) to ensure a smooth implementation. During this period, the manufacturer has to adapt the product to the CRA requirements, if needed, and perform the conformity assessment described in this chapter.

Module H might be helpful for manufacturers of important and critical products that place numerous types or models on the market since it provides a holistic system that streamlines the conformity assessment.

6.5 Which evaluation methodology should a manufacturer apply?

The CRA does not mandate the use of any specific evaluation methodology, potentially including testing. However, typically the application of an appropriate harmonised standard or technical specification is common practice by manufacturers.

The manufacturer can perform the relevant tests or testing procedures in their own laboratories, if available, or in external ones. The CRA does not lay down any specific requirements on laboratories performing the tests related to the conformity assessment procedures. The manufacturer assumes the sole responsibility for the conformity assessment.

The market surveillance authorities might perform tests or evaluation procedures during the relevant inspections. In this regard, they might consider applying the same methodology as the one used by the manufacturer, especially if that methodology is part of harmonised standard in support of the CRA. This being said, the market surveillance authority may apply a different methodology, on a justified basis. It must be highlighted that cybersecurity testing is not deterministic as in other NLF-regulated fields and the results might not be unique.

6.6 What is the technical documentation?

The technical documentation must contain the elements laid down in Annex VII of the CRA.

The manufacturer must take into consideration that the technical documentation is not only an internal deliverable but it might be requested by the market surveillance authorities. Therefore, it has to be comprehensive and clear. The manufacturer must be able to demonstrate that the product has been designed, developed and manufactured to comply with the essential requirements of the CRA. The latter includes specifications of vulnerability handling processes.

The technical documentation can be written in any language. Nevertheless, if it is required by a market surveillance authority, it needs to be provided in a language easily understood by this authority.

There is no obligation to make the technical documentation available to a manufacturer's customers or to the public, with the exception of manufacturers of free and open-source software that fall under the categories set out in Annex III (important products of class I or II) that wish to self-attest their conformity, in accordance with Article 32(5).

6.7 What is the CE marking?

The CE marking is a simple visual self-declaration of the manufacturer that the product is compliant with all the applicable NLF pieces of legislation and, in particular, with the CRA. It is addressed to consumers and market surveillance authorities. It is regulated in Articles 29 and 30. Further information can also be found in section 4.5.1. of the Blue Guide.

Products must bear the CE marking in a visible, legible and indelible way. As a general rule, it has to be larger than 5 mm. Exceptions can be accepted when the size of the product does not allow it, provided that it remains visible. The CE marking cannot have a size less than 5 mm on the grounds of aesthetic reasons.

The CE marking cannot be affixed in a part of the product that is not easily visible according to its intended use.

Software products also need to bear the CE marking. In accordance with Article 30(1), for software products the CE marking shall be affixed either to the EU declaration of conformity or on the website accompanying the software product. In the latter case, the relevant section of the website shall be easily and directly accessible to consumers.

The CE marking cannot be affixed if the manufacturer has not performed a conformity assessment procedure, with a positive result.

6.8 What is the declaration of conformity?

The declaration of conformity is a document in which the manufacturer declares that the product is compliant with the CRA, and assumes responsibility for that.

The declaration of conformity must accompany the product placed on the market. Two formats are allowed:

- The full declaration of conformity, following the template laid down in Annex V.
- A simplified declaration of conformity, which is a sentence whose template is laid down in Annex VI and that includes the internet address where the full declaration of conformity can be accessed.

The declaration of conformity is a document linked to the individual product and not only to the type or model. In this regard, it is not needed that it includes the unique identifier of the product. Nevertheless, a new version of the product might need a new declaration of conformity, especially when it implements a substantial modification.

The declaration of conformity cannot be signed if the manufacturer has not performed one of the relevant conformity assessment procedures, with a positive result.

In accordance with Article 28(3) and as stated in section 4.4 of the Blue Guide, where several pieces of Union harmonisation legislation apply to a product, the manufacturer or the authorised representative has to provide a single declaration of conformity in respect of all such Union acts. In order to reduce the administrative burden on economic operators and facilitate its adaptation to the modification of one of the applicable Union acts, the single declaration may be a dossier made up of relevant individual Declarations of conformity.

6.9 What are notified bodies?

Notified bodies are private or public entities that examine products to ensure that they comply with the CRA. Their competence is assessed by notifying authorities of Member States and the list is available on the NANDO system.

Notified bodies have to be independent vis-à-vis the manufacturers and the market surveillance authorities, to avoid any conflict of interest.

6.10 When will harmonised standards to support CRA compliance be ready?

The Commission standardisation request (M/606) addressed to CEN, CENELC and ETSI foresees the development of a set of harmonised standards to support CRA compliance,

distinguishing between horizontal (product-agnostic) standards and vertical (product-specific) standards.

Horizontal standards are meant to provide a coherent generic framework, methodology and taxonomy to support the development of further, granular vertical harmonised standards for specific products or product types, as well as to support manufacturers in defining and implementing the security requirements applicable to their respective products. The Commission requested the development of 15 horizontal standards, which the European Standardisation Organisations (ESOs) have clustered in 3 deliverables:

- A harmonised European standard on designing, developing and producing products with digital elements in such a way that they ensure an appropriate level of cybersecurity based on the risks, to be adopted by the ESOs by 30 August 2026;
- A harmonised European standard covering the essential cybersecurity requirements relating to the properties of products with digital elements as set out in Part I of Annex I, to be adopted by the ESOs by 30 October 2027;
- A harmonised European standard on vulnerability handling for products with digital elements, to be adopted by the ESOs by 30 August 2026.

Vertical standards are meant to be product specific and to cover a specific set of risks appropriate to a particular intended purpose and reasonably foreseeable use. The Commission requested the development of 26 vertical standards (which the ESOs are addressing through 31 separate deliverables) to be adopted by the ESOs by 30 October 2026. The vertical standards under development cover the categories of important and critical products with digital elements set out in Annexes III and IV of CRA.

In accordance with Article 27(6), where a harmonised European standard is adopted by the ESOs, the Commission shall assess it in accordance with Regulation (EU) No 1025/2012 for the purpose of publishing its reference in the Official Journal of the European Union.

7 Transition period

7.1 When does the CRA start applying?

According to Article 71(2) Articles 35 to 51 apply from 11 June 2026. Member States are required to designate by that date notifying authorities that are responsible for setting up and carrying out the necessary procedures for the assessment, designation and notification of conformity assessment bodies.

Reporting obligations laid down in Article 14 apply from 11 September 2026. As of that date, manufacturers are required to notify actively exploited vulnerabilities and severe incidents having an impact on the security of their products with digital elements via the single reporting platform.

The obligations of manufacturers to ensure that products with digital elements are in conformity with the essential cybersecurity requirements set out in Annex I, the provisions on market surveillance and enforcement, as well as all the other provisions set out in the CRA, apply from 11 December 2027.

According to Article 69(1), EU-type examination certificates and approval decision issued regarding cybersecurity requirements for products with digital elements that are subject to other Union harmonisation legislation, such as Commission Delegated Regulation (EU) 2022/30, remain valid until 11 June 2028 (unless otherwise specified in such legislation or unless the certificate expires before that date).

7.2 A manufacturer develops a product type before the CRA applies. Can it continue to manufacture products identical to that type after the CRA applies?

As stated in section 2.2 of the Blue Guide, Union harmonisation legislation including the CRA applies to individual products, and not product types. Therefore, only individual products that have been placed on the market before 11 December 2027 do not need to comply with the CRA.

Products that are manufactured according to a type that is not compliant with the CRA cannot be placed on the market on or after 11 December 2027, even if the first instance of that product "type" has been placed on the market before 11 December 2027.

For example, a manufacturer has produced 10 000 copies of a router according to a type that is not compliant with the CRA. It places those 10 000 copies on the market before 11 December 2027. Even if those units have not reached their final user (but have been placed on the market), the manufacturer does not need to bring them into compliance with the CRA (see also entry *1.4 Does the CRA apply to products with digital elements*

placed on the market before 11 December 2027?). However, that manufacturer may not produce another 5 000 copies of that router and place them on the market after 11 December 2027, as those 5 000 copies would not be compliant with the CRA.

7.3 Can a manufacturer place on the market products with digital elements developed during the transition period, and that integrate components that do not bear the CE marking?

> *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* (Article 13(5)).
>
> *Immediately after the transitional period for the application of this Regulation, a manufacturer of a product with digital elements that integrates one or several components sourced from third parties which are also subject to this Regulation may not be able to verify, as part of its due diligence obligation, that the manufacturers of those components have demonstrated conformity with this Regulation by checking, for instance, if the components already bear the CE marking. This may be the case where the components have been integrated before this Regulation becomes applicable to the manufacturers of those components. In such a case, a manufacturer integrating such components should exercise due diligence through other means* (Recital 35).

As explained in the entries *4.4.1 What does the CRA prescribe when integrating components?* and *4.4.3 In order to exercise due diligence, should a manufacturer only integrate components that bear the CE marking?*, a manufacturer can integrate components that do not bear the CE marking, but is required to exercise due diligence to ensure that those components do not compromise the cybersecurity of its product with digital elements.

During the transition period before the CRA applies, manufacturers will not be able to check whether third-party components are compliant with the CRA. This does not prevent manufacturers from integrating such components, and they should exercise due diligence through other means (see also entry *4.4.2 What is the appropriate level of due diligence?*).

7.4 Is a manufacturer allowed to integrate components that are important or critical products with digital elements that do not follow harmonised standards?

Yes, manufacturers are free to integrate components that are important or critical products that have not been designed in accordance with harmonised standards – regardless of whether such harmonised standards are available or not.

The application of harmonised standards is a means to demonstrate compliance, but is not the only means to do so.

Furthermore, as discussed in entries *4.4.1 What does the CRA prescribe when integrating components?* and *4.4.3 In order to exercise due diligence, should a manufacturer only integrate components that bear the CE marking?*, the manufacturer is not required to integrate only components that bear the CE marking.

7.5 Are distributors required to bring into compliance products with digital elements placed on the market before 11 December 2027?

No, products with digital elements placed on the market before 11 December 2027 are not subject to the requirements of the CRA (with the exception of reporting obligations), unless they are substantially modified. Distributors are therefore not required to bring such products into compliance with the CRA on or after 11 December 2027, unless they carry out a substantial modification.