Ministry of Economic Affairs

Guide Cyber Resilience Act

Version 2.0

Table of contents

Reading guide en disclaimer
You are a manufacturer, importer or distributor of a product with digital elements. If so, you will have to be compliant with the Cyber Resilience Act. This guide had been prepared for you, a tool to help you understand the most important aspects of the Cyber Resilience Act in an accessible way. No rights can be derived from the contents of this guide. The legal text of the Cyber Resilience Act always remains leading.

Do you have any feedback for improving this guide?
Please email teamcra@minezk.nl. Your feedback will be used to improve this guide.

Are you reading a printed version of this guide?
You can always find the latest version at www.ondernemersplein.overheid.nl.

The Cyber Resilience Act

The Cyber Resilience Act (CRA) is a European regulation that focuses on improving the security of products with digital elements. Users in the European Union (EU) must be able to trust that products are digitally secure. Under the CRA, digital products must meet essential security requirements and must be kept secure throughout their expected lifetime through security updates. This ensures that consumers and businesses can use digital products safely.

On December 10, 2024, the CRA came into effect, marking the start of a phased implementation period lasting a total of three years. During this period, technical standards will be developed and manufacturers will be given time to take the CRA requirements into account during the development of products with digital elements. From September 11, 2026, the obligation to report actively exploited vulnerabilities and incidents will come into force. From December 11, 2027, all requirements will come into force and all products with digital elements that are made available on the European market must comply with the CRA.[1]

The full text of the regulation can be found here.[2]

What does the Cyber Resilience Act mean for your organisation?

The CRA applies to products with digital elements that are made available on the European market and divides them into four different types of products. Some products with digital elements are exempted, for example because they are already covered by other legislation. It is important to determine whether you place the product with digital elements on the European market as a manufacturer, importer, or distributor. Depending on the type of product and what type of economic operator you are, different obligations apply.

[1] Wireless connected devices (such as laptops, smart doorbells, etc.) will already be required to comply with cybersecurity requirements under the Radio Equipment Directive from August 2025 onwards.

[2] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202402847.

Glossary[3]

Product with digital elements: a software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately.

Remote data processing: 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.

Manufacturer: a natural or legal person who develops or manufactures products with digital elements or has products with digital elements designed, developed or manufactured, and markets them under its name or trademark, whether for payment, monetisation or free of charge.

Importer: a natural or legal person established in the Union who places on the market a product with digital elements that bears the name or trademark of a natural or legal person established outside the Union.

Distributor: a natural or legal person in the supply chain, other than the manufacturer or the importer, that makes a product with digital elements available on the Union market without affecting its properties.

Substantial modification: a change to the product with digital elements following its placing on the market, which affects the compliance of the product with digital elements with the essential cybersecurity requirements set out in Part I of Annex I or which results in a modification to the intended purpose for which the product with digital elements has been assessed.

Intended purpose: 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.

Reasonably foreseeable use: 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.

[3] Article 3 Cyber Resilience Act (Definitions).

CE marking: a marking by which a manufacturer indicates that a product with digital elements and the processes put in place by the manufacturer are in conformity with the essential cybersecurity requirements set out in Annex I and other applicable Union harmonisation legislation providing for its affixing.

Conformity assessment: the process of verifying whether the essential cybersecurity requirements set out in Annex I have been fulfilled.

Actively exploited vulnerability: a vulnerability for which there is reliable evidence that a malicious actor has exploited it in a system without permission of the system owner.

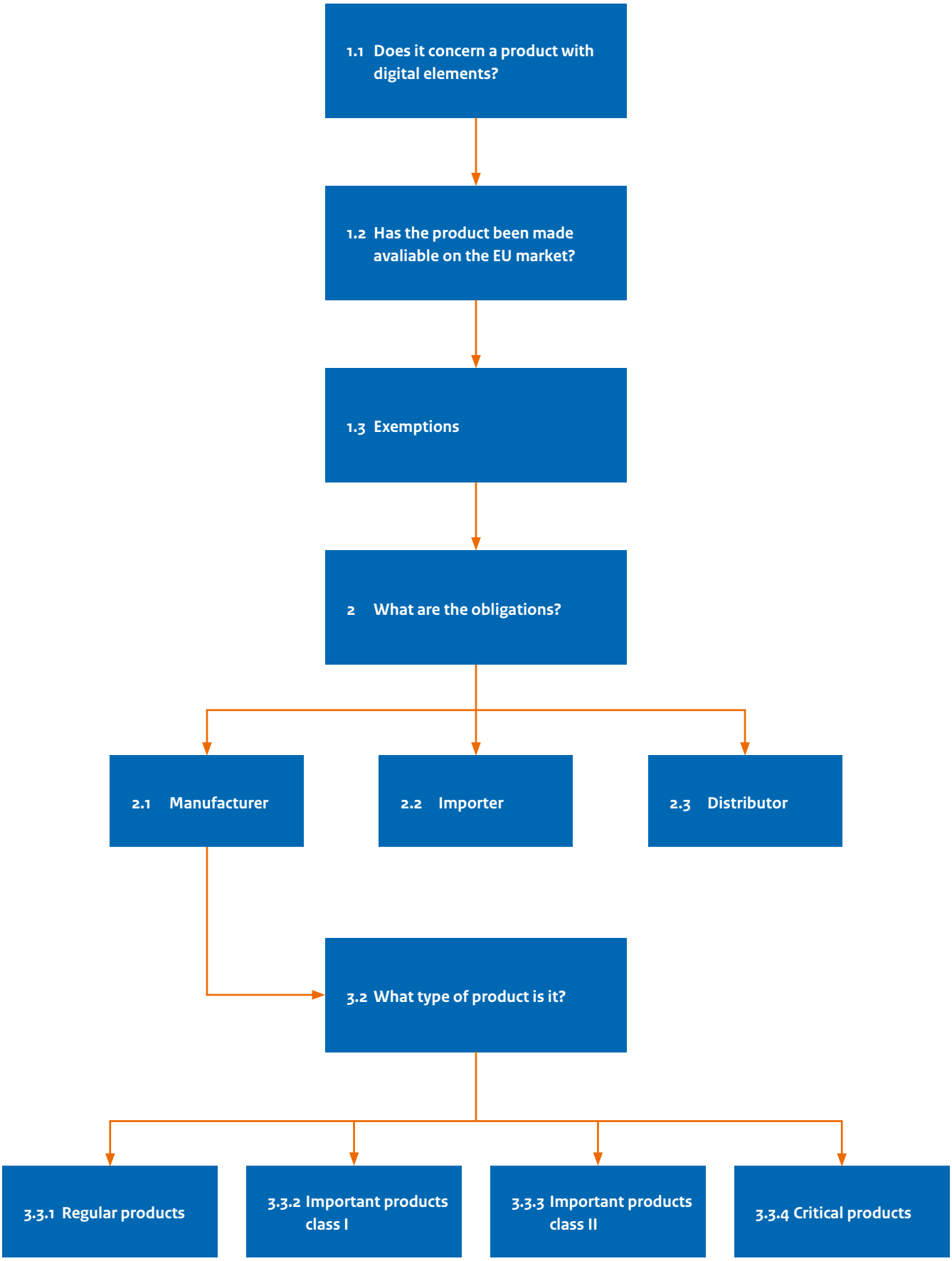
Incident having an impact on the security of the product with digital elements: an incident that negatively affects or is capable of negatively affecting the ability of a product with digital elements to protect the availability, authenticity, integrity or confidentiality of data or functions.

Support period: the period during which a manufacturer is required to ensure that vulnerabilities of a product with digital elements are handled effectively and in accordance with the essential cybersecurity requirements set out in Part II of Annex I.

Vulnerability: a weakness, susceptibility or flaw of a product with digital elements that can be exploited by a cyber threat.

Harmonised standard: a harmonised standard as defined in Article 2, point (1)(c), of Regulation (EU) No 1025/2012.

Conformity assessment body: a conformity assessment body as defined in Article 2, point (13), of Regulation (EC) No 765/2008.


1.1 Does it concern a product with digital elements?
1.2 Has the product been made avaliable on the EU market?
1.3 Exemptions
2 What are the obligations?
2.1 Manufacturer
2.2 Importer
2.3 Distributor
3.2 What type of product is it?
3.3.1 Regular products
3.3.2 Important products class I
3.3.3 Important products class II
3.3.4 Critical products

1 Scope of the Cyber Resilience Act

1.1 Does it concern a product with digital elements?

In principle, the Cyber Resilience Act (CRA) applies to all **products with digital elements** that are made available on the European Union (EU) market. Products with digital elements include all software and hardware products and associated solutions for **remote data processing**. Services are not covered by the CRA. A solution for remote data processing is only covered by the CRA if it is essential to the functionality of a product with digital elements that is covered by the CRA. Separate software and hardware components are also covered by the CRA.

1.2 Has the product been made available on the EU market?

The CRA applies to products with digital elements that are placed on the EU market. This means that the CRA covers products with digital elements when they are made available on the market in the EU for the first time. To be within scope of the CRA, a product with digital elements must be offered commercially as part of a commercial activity. Non-commercially offered (open-source) software or products developed for internal use are not covered by the CRA.

The obligations of the CRA are linked to the offering of a product with digital elements on the market and therefore only apply in situations where the product is offered commercially.

1.3 Exemptions

Various products with digital elements are already regulated by other sector-specific cybersecurity requirements and are therefore not covered by the CRA. This is the case for medical devices, motor vehicle products, civil aviation products, and marine equipment.[4] The CRA also does not apply to spare parts that function exactly the same as the original, or products developed exclusively for national security, defence, or classified information processing purposes.

[4] Article 2 (2) CRA lists the specific regulations and directives to which the exceptions apply.

2 What are the obligations?

The Cyber Resilience Act (CRA) mentions three market participants: the manufacturer, the importer and the distributor. A **manufacturer** develops or manufactures products, or has products designed, developed, or manufactured, and markets them under its own (brand) name. An **importer** is established in the European Union (EU) and markets a product bearing the (brand) name of a party established outside the EU. A **distributor** is a party in the supply chain other than the manufacturer or importer, who offers a product on the EU market without affecting its characteristics. Importers or distributors who market a product under their own name or make a **substantial modification** to a product are also considered manufacturers under the CRA.

The CRA imposes obligations on manufacturers, and by extension on importers and distributors. Economic operators must ensure that products with digital elements (continue to) meet certain requirements and are also required to account for compliance with these requirements. This is done through various documentation and reporting obligations.

2.1 I am a manufacturer

A manufacturer is a natural or legal person who manufactures a product (or has it designed and manufactured) and then markets it under their own name or trademark. As a manufacturer, you have the same obligations whether you are based in the EU or outside it. You must take the CRA into account from the design stage onwards.

The CRA imposes the following obligations on manufacturers:

- When designing, developing, and manufacturing the product, ensure that the product meets the essential cybersecurity requirements. Section 3.1 of this guide discusses the essential cybersecurity requirements as set out in Annex I to the CRA in more detail. To this end, a cybersecurity risk assessment must be carried out:
  - the manufacturer shall first assess the cybersecurity risks associated with the product;
  - the manufacturer takes this cybersecurity risk assessment into account during the planning, design, development, production, delivery, and maintenance phases of the product in order to minimise cybersecurity risks, prevent incidents, and limit their consequences as much as possible;
  - the cybersecurity risk assessment shall include at least an analysis of cybersecurity risks based on the **intended purpose** and **reasonably foreseeable use**, as well as the conditions of use, of the product with digital elements, such as the operating environment or the assets to be protected, taking into account the expected lifetime of the product;
  - the assessment of cybersecurity risks shall indicate whether, and if so how, the security requirements set out in Part I, point 2, of Annex I to the CRA apply to the digital element product concerned and how those requirements are implemented on the basis of the assessment of cybersecurity risks;
  - it shall also indicate how the manufacturer applies Part I, point 1, of Annex I, and the requirements on vulnerability response set out in Part II of Annex I to the CRA;
  - the cybersecurity risk assessment shall be documented and, where necessary, updated during the support period;
  - where applicable: with regard to integrated components from third parties, a manufacturer shall act with due care, namely that the manufacturer verifies that the integrated components from third parties do not compromise the safety of the product they place on the market. Components are also products that must comply with the CRA, so the **CE marking** can be used as a reference. For components that are not sold separately on the market, which may be the case for open-source components in particular, the manufacturer must verify this in another way.
- Record the cybersecurity risks of the product in the technical documentation.
- Perform a **conformity assessment** to verify that the product meets the essential cybersecurity requirements.

- Add the following information to the product with digital elements:
  - The type, batch, or serial number.
  - The visible, legible, and indelible CE marking (unless not possible or justified, on the packaging).
- Add the following information to the product packaging or a document accompanying the product:
  - The name, registered trade name, or registered trademark.
  - The postal address, email address, or other digital details.
  - The website where the manufacturer can be contacted.
- Determining the expected use time and stating the end of the support period at the time of purchase by means of the month and year.

2.1.1 *Vulnerability handling*

Once users have started using the products, the product must be kept secure throughout its expected use time, taking into account reasonable user expectations, the nature of the product, its intended purpose, as well as relevant EU law determining the lifetime of products with digital elements. The **support period** must be at least five years, unless the expected use time is shorter.

If a **vulnerability** is discovered, a free security update must be offered as soon as possible. Only in the case of customised solutions for business customers it may contractually be agreed on that costs will be charged for vulnerability response.

Products must be offered with the setting that updates are installed automatically in principle, with an opt-out option if automatic updating is not desired by the user. Products for industrial environments are not required to install updates automatically, as this would be undesirable.

2.1.2 *Reporting obligation*

Manufacturers must report any actively exploited vulnerabilities or severe incidents that affect the security of the product. This applies to both patched and unpatched vulnerabilities. From September 11, 2026, manufacturers of products with digital elements must report the actively exploited vulnerabilities or severe incidents via the single reporting platform of the National Cyber Security Center.[5] This report is also accessible to ENISA (European Network and Information Security Agency).

In the case of an **actively exploited vulnerability**, the following information must be reported within the applicable deadlines:

- Without undue delay and in any event within 24 hours after the manufacturer has become aware of it: an early warning, stating:
  - the actively exploited vulnerability;
  - where applicable, the Member States of which the manufacturer is aware the product has been made available.

- Within 72 hours after the manufacturer becomes aware: a vulnerability notification, containing general information, where available, about:
  - the product with digital elements concerned;
  - the general nature of the exploit and of the vulnerability concerned;
  - any corrective or mitigating measures (patch) taken;
  - corrective or mitigating measures that users can take;
  - where applicable: how sensitive the manufacturer considers the reported information to be.

[5] This applies to manufacturers whose EU headquarters are located in the Netherlands. The regulation assumes that this is the case when decisions regarding the cybersecurity of its product with digital elements are mainly taken in the Netherlands. If the main place of business cannot be determined in this way, the Member State where the manufacturer has the establishment with the largest number of employees in the Union is decisive: if this is the Netherlands, the manufacturer must report to the NCSC. If the manufacturer has its headquarter in another Member State, the manufacturer had the obligation to report in that Member State.

- Within 14 days after a corrective or mitigation measure (patch) is available: a final report, containing at least the following information:
  - description of the vulnerability, including its severity and consequences;
  - if available: information about the malicious actor who exploited the vulnerability;
  - details about the security update or other corrective measures that have been made available to remedy the vulnerability.

For any severe **incident that affects the security of the product with digital elements**, the following information must be reported within the applicable deadlines:

- Without undue delay and in any case within 24 hours after the manufacturer has become aware of it: an early warning, stating:
  - whether the incident is suspected of being caused by unlawful or malicious acts;
  - where applicable, the Member States in which the manufacturer knows the product has been made available.
- Within 72 hours after the manufacturer becoming aware: an incident notification, containing general information, to the extent available, on:
  - the nature of the incident;
  - an initial assessment of the incident;
  - any corrective or mitigation measures taken (patch);
  - corrective or mitigation measures that users can take;
  - where applicable: how sensitive the manufacturer considers the notified information to be.
- Within one month of submitting the incident report: a final report containing at least the following information:
  - a detailed description of the incident, including its severity and impact;
  - the type of threat or root cause that is likely to have triggered the incident;
  - applied and ongoing mitigation measures.

The reporting obligation under the CRA applies to all products with digital elements made available on the EU market, including those already on the market before December 11, 2027.

2.2 I am an importer

An importer is a natural or legal person established in the EU who places a product from a country outside the EU on the EU market. As an importer, you must ensure that the manufacturer has fulfilled all obligations relating to the product you place on the market.

In order to place a product with digital elements on the market, the importer must ensure that:

- the manufacturer has followed the correct procedure for conformity assessment;
- the manufacturer has drawn up the technical documentation, affixed the CE marking, and fulfilled all traceability obligations (indication of the manufacturer's contact details, type, batch or serial number of the product);
- the product is accompanied by the necessary instructions and safety information in a language that is easily understandable to consumers and other end users;
- your name, trade name or trademark and contact address are clearly indicated on the product, packaging or documentation.

Only products with digital elements that meet the essential cybersecurity requirements, where the vulnerability handling process established by the manufacturer comply with the essential cybersecurity requirements, may be made available on the EU market. Where the importer knows or has reason to believe that a product or the vulnerability handling process established by the manufacturer does not comply with the CRA, the product may not be made available on the market until the manufacturer has

remedied the situation. If the product poses a significant cybersecurity risk, the importer must notify the manufacturer and the supervisory authority/Dutch Authority for Digital Infrastructure.

The importer must also ensure that necessary corrective measures are taken if the product has already been made available on the market, such as bringing it into compliance with the regulations, recalling it, or withdrawing it from the market. Importers who become aware of a vulnerability in a product must also notify the manufacturer without undue delay.

2.3 I am a distributor

A distributor is a natural or legal person in the supply chain who places a product on the EU market that they have obtained from a manufacturer, importer, or another distributor. As a distributor, you must ensure that the product with digital elements complies with the CRA obligations when you place it on the market.

Before offering a product with digital elements on the market, the distributor carefully checks that:

- the product with digital elements bears the CE marking;
- the product with digital elements is accompanied by technical documentation and the EU declaration of conformity.

3 Cybersecurity requirements for products that are made available on the EU market

3.1 Essential cybersecurity requirements

Products with digital elements must meet the cybersecurity requirements listed in Annex 1 of the CRA before they are made available on the market in the EU. These requirements are divided into:

Part I Cybersecurity requirements relating to the properties of products with digital elements

1. Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks.
2. On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall:
   a. be made available on the market without known exploitable vulnerabilities;
   b. 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;
   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;
   d. ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible unauthorised access;
   e. protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state of the art mechanisms, and by using other technical means;
   f. protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, and report on corruptions;
   g. process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended purpose of the product with digital elements (data minimisation);
   h. protect the availability of essential and basic functions, also after an incident, including through resilience and mitigation measures against denial-of-service attacks;
   i. minimise the negative impact by the products themselves or connected devices on the availability of services provided by other devices or networks;
   j. be designed, developed and produced to limit attack surfaces, including external interfaces;
   k. be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques;
   l. provide security related information by recording and monitoring relevant internal activity, including the access to or modification of data, services or functions, with an opt-out mechanism for the user;
   m. provide the possibility for users to securely and easily remove on a permanent basis all data and settings and, where such data can be transferred to other products or systems, ensure that this is done in a secure manner.

Part II Vulnerability handling requirements

Manufacturers of products with digital elements shall:

1. identify and document vulnerabilities and components contained in products with digital elements, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the products;
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;
3. apply effective and regular tests and reviews of the security of the product with digital elements;
4. once a security update has been made available, share and publicly disclose information about fixed **vulnerabilities**, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and clear and accessible information helping users to remediate the vulnerabilities; in duly justified cases, where manufacturers consider the security risks of publication to outweigh the security benefits, they may delay making public information regarding a fixed vulnerability until after users have been given the possibility to apply the relevant patch;
5. put in place and enforce a policy on coordinated vulnerability disclosure;
6. take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third-party components contained in that product, including by providing a contact address for the reporting of the vulnerabilities discovered in the product with digital elements;
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;
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.

As stated in section 2.1 of this guide, the obligations apply to manufacturers, while the derived obligations that apply to importers and distributors are included in sections 2.2 and 2.3 of this guide, respectively. Importers and distributors must verify that a manufacturer has ensured that the product complies with these requirements, so that products from outside the EU also comply with these requirements.

Once the product is put into use, products with digital elements must be kept secure throughout their expected lifetime.

3.1.1 *Conformity assessment*

Manufacturers use a conformity assessment to check whether the product with digital elements complies with the cybersecurity requirements listed in Annex 1 to the CRA (see also section 3.1 of this guide) before it is made available on the EU market. The conformity assessment must be carried out during the design phase and continues in the production phase. Even if you have your products designed or manufactured by others, you are responsible for the conformity assessment. The aim is for manufacturers to minimise cybersecurity risks, prevent incidents, and minimise the consequences of incidents.

The information about the conformity assessment must be included in the technical documentation.

The technical documentation shall contain at least the following information, as applicable to the product with digital elements in question:

1. a general description of the product with digital elements, including:
   a. its intended purpose;
   b. versions of software affecting compliance with essential cybersecurity requirements;
   c. where the product with digital elements is a hardware product, photographs or illustrations showing external features, marking and internal layout;
   d. user information and instructions as set out in Annex II;
2. a description of the design, development and production of the product with digital elements and vulnerability handling processes, including:
   a. necessary information on the design and development of the product with digital elements, including, where applicable, drawings and schemes and a description of the system architecture explaining how software components build on or feed into each other and integrate into the overall processing;
   b. necessary information and specifications of the vulnerability handling processes put in place by the manufacturer, including the software bill of materials, the coordinated vulnerability disclosure policy, evidence of the provision of a contact address for the reporting of the vulnerabilities and a description of the technical solutions chosen for the secure distribution of updates;
   c. necessary information and specifications of the production and monitoring processes of the product with digital elements and the validation of those processes;
3. an assessment of the cybersecurity risks against which the product with digital elements is designed, developed, produced, delivered and maintained pursuant to Article 13, including how the essential cybersecurity requirements set out in Part I of Annex I are applicable;
4. relevant information that was taken into account to determine the support period pursuant to Article 13(8) of the product with digital elements;
5. a list of the harmonised standards applied in full or in part the references of which have been published in the Official Journal of the European Union, common specifications as set out in Article 27 of this Regulation or European cybersecurity certification schemes adopted pursuant to Regulation (EU) 2019/881 pursuant to Article 27(8) of this Regulation, and, where those harmonised standards, common specifications or European cybersecurity certification schemes have not been applied, descriptions of the solutions adopted to meet the essential cybersecurity requirements set out in Parts I and II of Annex I, including a list of other relevant technical specifications applied. In the event of partly applied harmonised standards, common specifications or European cybersecurity certification schemes, the technical documentation shall specify the parts which have been applied;
6. reports of the tests carried out to verify the conformity of the product with digital elements and of the vulnerability handling processes with the applicable essential cybersecurity requirements as set out in Parts I and II of Annex I;
7. a copy of the EU declaration of conformity;
8. where applicable, the software bill of materials, further to a reasoned request from a market surveillance authority provided that it is necessary in order for that authority to be able to check compliance with the essential cybersecurity requirements set out in Annex I.

3.1.2 *Technical standard*

The cybersecurity requirements referred to in section 2.1 of this guide, as set out in Annex 1 to the CRA, are translated by CEN/CENELEC and ETSI into specific technical standards that enable a product to comply with the requirement. When the EC approves a standard, it becomes a **harmonised standard**. These standards can be used by manufacturers in the conformity assessment of regular products and important class 1 products. The different types of products covered by the CRA are explained in the following section.

3.2 What type of product is it?

The Cyber Resilience Act (CRA) distinguishes between four different types of products:

1. Regular products,
2. Important products class 1,
3. Important products class 2, and
4. Critical products.

The main rule is that a manufacturer may perform the conformity assessment itself. This may be different in the case of an important product with digital elements. Products with digital elements that are classified as critical products must always be assessed by a conformity assessment body.

3.2.1 *Regular products*

Regular products are defined as all products with digital elements that are not classified as important or critical in Annexes 3 and 4 of the CRA. These include, for example, mobile apps, video games, or network equipment. A self-assessment may be applied to these products.

3.2.2 *Important products class 1*

Appendix 3 to the CRA lists the important products with digital elements. The important products are divided into two classes.

The following products fall into the first class:

1. identity management systems and privileged access management software and hardware, including authentication and access control readers, including biometric readers
2. standalone and embedded browsers
3. password managers
4. software that searches for, removes, or quarantines malicious software products with digital elements with the function of virtual private network (VPN)
5. network management systems
6. security information and event management (SIEM) systems
7. boot managers
8. public key infrastructure and digital certificate issuance software
9. physical and virtual network interfaces
10. operating systems
11. routers, modems intended for the connection to the internet, and switches
12. microprocessors with security-related functionalities
13. microcontrollers with security-related functionalities
14. application specific integrated circuits (ASIC) and field-programmable gate arrays (FPGA) with security-related functionalities
15. smart home general purpose virtual assistants

16. smart home products with security functionalities, including smart door locks, security cameras, baby monitoring systems and alarm systems
17. toys connected to the internet covered by the To Safety Directive that have social interactive features (e.g. speaking or filming) or that have location tracking features
18. personal wearables that are intended to be worn or placed on the human body and are intended for health monitoring (such as tracking) (and are not in vitro diagnostic medical devices), or personal wearables that are intended for use by and for children

Self-assessment of these products may only be based on harmonised standards. Where no harmonised European standard exists, the product with digital elements must be assessed by a **conformity assessment body**.

3.2.3 *Important products class 2*

In the second class of Annex 3 to the CRA, the following are considered important products:

1. hypervisors and container runtime systems that support virtualised execution of operating systems and similar environments
2. firewalls, intrusion detection and prevention systems
3. tamper-resistant microprocessors
4. tamper-resistant microcontrollers

These products with digital elements must always be assessed by a conformity assessment body before they are made available on the EU market.

3.2.4 *Critical products*

Annex 4 to the CRA lists the critical products with digital elements. These are:

1. hardware devices with security boxes
2. smart meter gateways within smart metering systems and other devices for advanced security purposes, including for secure cryptoprocessing
3. smartcards or similar devices, including secure elements

In the future, these critical products may be required to be certified under a suitable certification scheme under the Cyber Security Act. Until such a requirement is introduced, a critical product with digital elements must mandatorily undergo assessment by a conformity assessment body.

This brochure is published by:

Ministry of Economic Affairs
Bezuidenhoutseweg 73 | 2594 AC The Hague
P.O. Box 20401 | 2500 EK The Hague

September 2025 | 0925-108