

Cyber Resilience Act - CRA Guide Cyprus

A practical
introduction for
stakeholders

 **Stronger products
for a safer digital Europe**

 **Responsibilities across
the supply chain**

 **Cooperation for
resilience and trust**

 **Aligned with European values
and global best practices**



Prepared by the Digital Security Authority of Cyprus - NCCA

in collaboration with Working Group 4: EU and National Legislations of NCC-CY

Key Definitions

Some important terms used in CRA

Product with digital elements (PDE)

a software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately

Conformity Assessment

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

Logical Connection

a virtual representation of a data connection implemented through a software interface

Indirect Connection

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

Intended Purpose

the use for which a PDE is intended by the manufacturer, including the specific context & conditions of use, as specified in the information supplied by the manufacturer in the instructions for use, promotional/sales materials and statements and in the technical documentation

Remote data processing solutions

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 PDE from performing one of its functions

Cybersecurity Risk

the potential for loss or disruption caused by an incident and is to be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of the incident

Significant Cybersecurity Risk

a cybersecurity risk which, based on its technical characteristics, can be assumed to have a high likelihood of an incident that could lead to a severe negative impact, including by causing considerable material or non-material loss or disruption

1. Introductory Note

Why this guide was prepared

The Cyber Resilience Act (CRA) introduces a new European framework for the cybersecurity of products with digital elements. It applies to a wide range of hardware and software products placed on the EU market and introduces obligations for different actors in the supply chain, including manufacturers, authorised representatives, importers and distributors.

This guide has been prepared to support stakeholders in Cyprus in understanding the main requirements of the CRA and what they may need to do in practice. It is intended as an awareness and preparedness tool, not as a substitute for the Regulation itself or for legal advice.



What this guide is for

- understand what the CRA is and why it matters
- identify whether a product falls within scope
- understand the stakeholders affected and their respective roles under the Regulation
- recognise the key milestones and obligations
- understand the role of the relevant Cyprus authority
- help affected stakeholders plan their next actions related to CRA compliance



This guide is not



legal advice



a substitute for the CRA



a binding interpretation

2. What is the CRA?

A simple explanation

The CRA is an EU Regulation that sets cybersecurity requirements for products with digital elements. Its goal is to make hardware and software products placed on the EU market more secure throughout their lifecycle.

It introduces obligations for manufacturers and certain responsibilities for other actors in the supply chain, such as authorised representatives, importers and distributors.



**Secure-by-design
and by default**



**Security throughout
the product lifecycle**



**Vulnerability
handling and
reporting**



**Responsibilities
across the
supply chain**

CRA TIMELINE AT A GLANCE



10 Dec 2024

Entry into force



11 Jun 2026

Conformity
Assessment
Bodies can apply
for notification



11 Sep 2026

Reporting
obligations for
vulnerabilities and
cybersecurity
incidents start

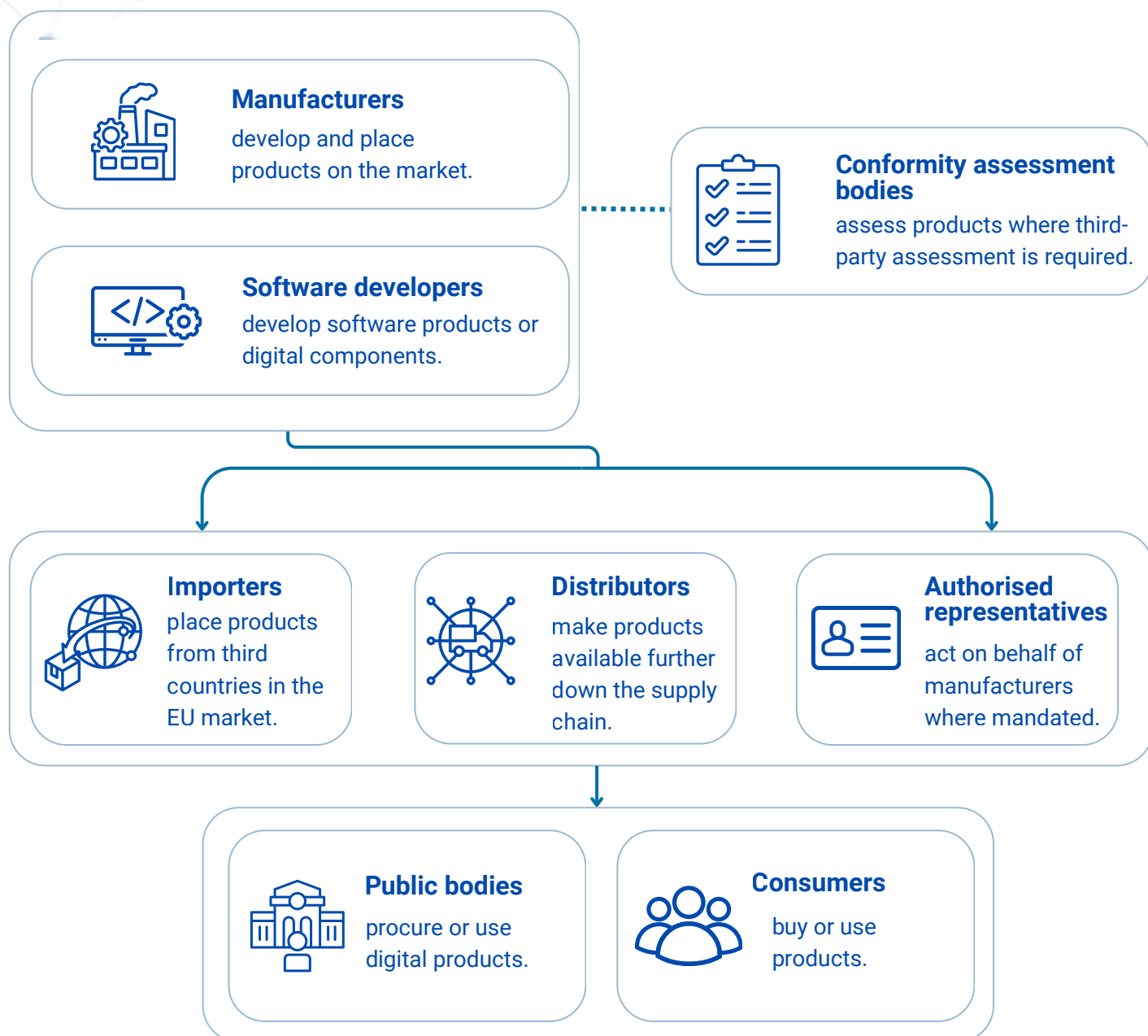


11 Dec 2027

Full application

3. Who this guide is for

A practical reference for stakeholders in Cyprus



How to use this guide

1. Find your role

Identify the stakeholder group that best matches your organisation.

2. Check if your product is in scope

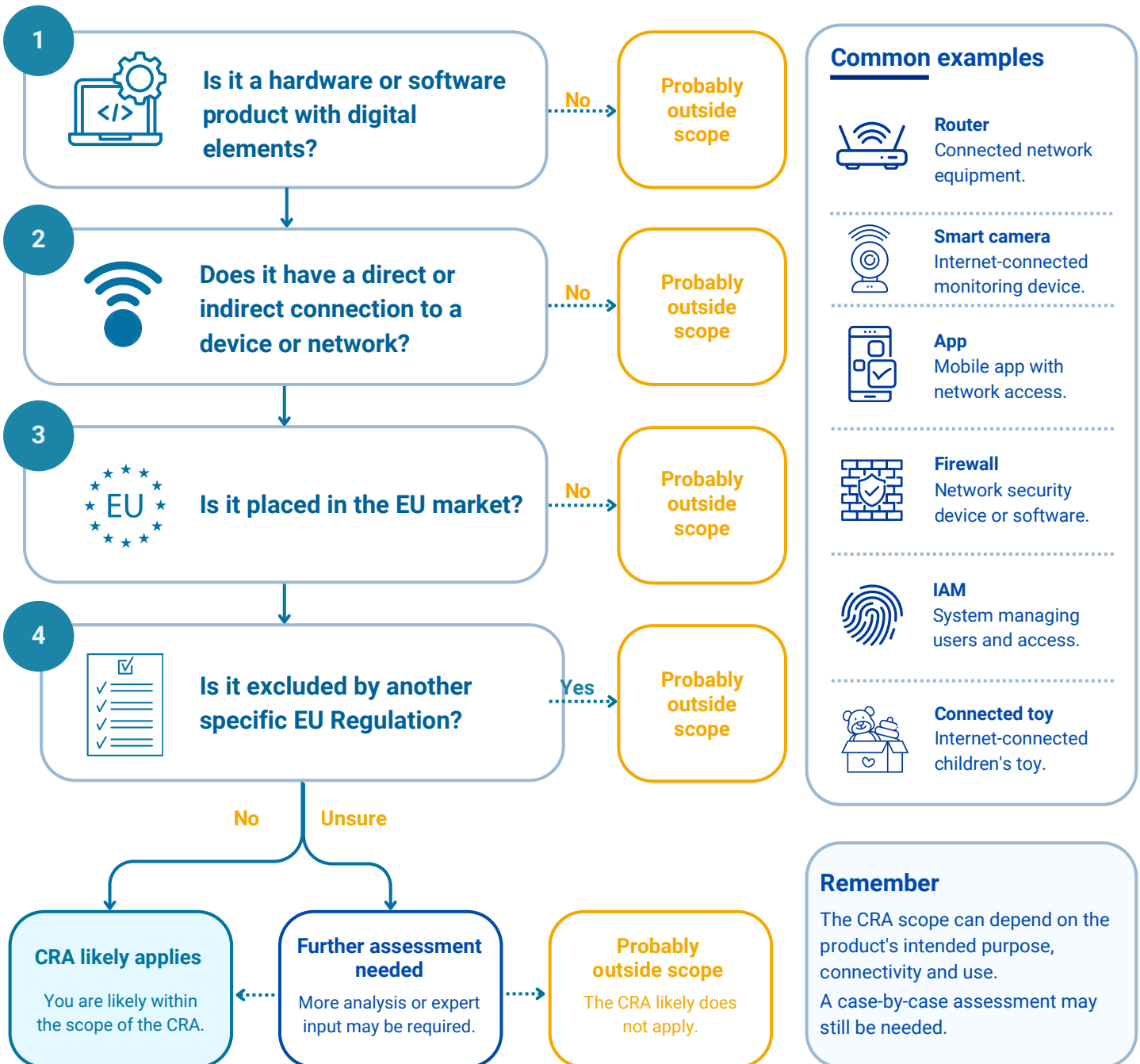
Use the guidance presented in Section 4 to understand whether the CRA applies.

3. Focus on the relevant obligations

Review the obligations that apply to your role and take action.

4. Does the CRA apply to my product?

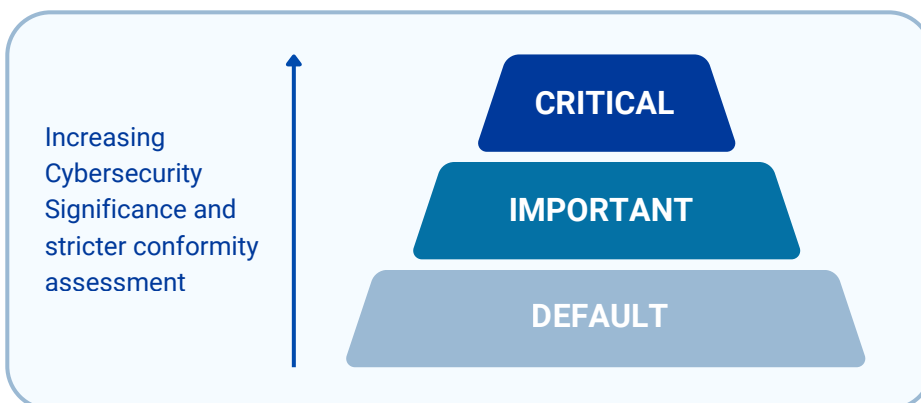
A simple decision flow



5. What type of product do I have?

Default, important and critical products under the CRA

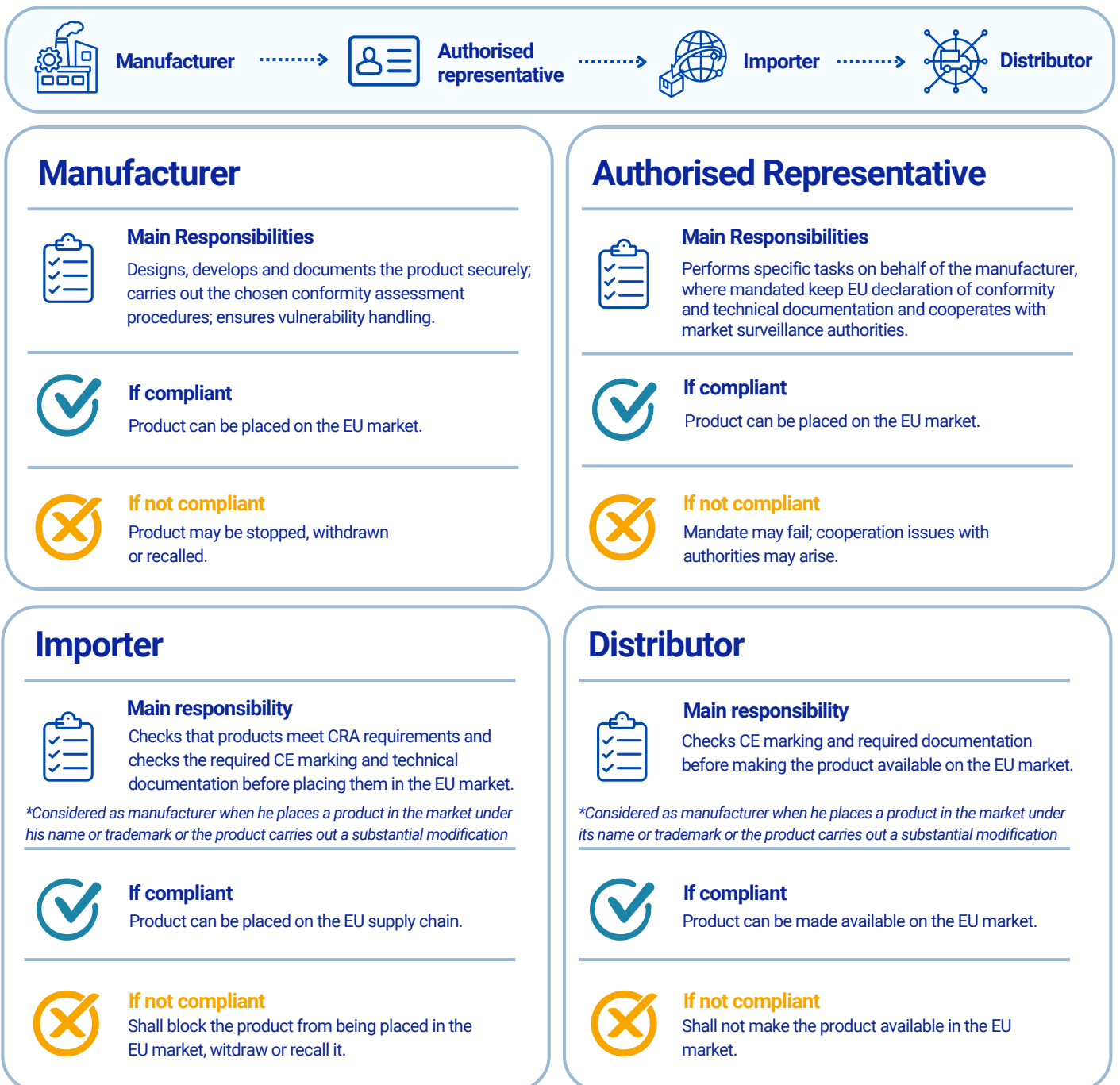
Once a product is within the scope of the CRA, the next step is to identify its category. In simple terms, products are grouped as default, important or critical. This matters because the product category can affect the level of scrutiny and the conformity assessment route.



The exact classification depends on the CRA and the product's functionality. If you are unsure, a more detailed assessment may be needed.

6. Responsibilities across the supply chain

Each economic operator has a role in ensuring that only CRA-compliant products enter and remain on the EU market



Non-compliance may lead to corrective actions, withdrawal, recall, restrictions, penalties and reputational damage.

7. Role of the Notifying Authority and Market Surveillance Authority in Cyprus

In Cyprus, the Digital Security Authority (DSA) is the designated authority for these CRA functions



Notifying Authority

Main Role

- ✓ Designates and notifies conformity assessment bodies (CABs).
- ✓ Assesses whether notified bodies meet the required competence, impartiality and independence criteria.
- ✓ Monitors notified bodies and takes action where requirements are no longer met.

Why it matters



Helps ensure that bodies involved in conformity assessment are trustworthy and competent.



Market Surveillance Authority

Main Role

- ✓ Checks whether products with digital elements placed on the market comply with the CRA.
- ✓ Requests information and documentation from economic operators where needed.
- ✓ Takes corrective action when products are non-compliant or present cybersecurity risks.
- ✓ Cooperates with other authorities and relevant EU mechanisms.

Why it matters



Helps ensure that only compliant products enter and remain on the EU market.



The CRA relies both on preventive oversight (through notified bodies) and on enforcement after products enter the market.



MORE INFORMATION

Website: www.ncca.cy

Email: info@ncca.ee.cy



Co-funded by
the European Union



NCC 
CYBERSECURITY NATIONAL
COORDINATION CENTRE
CYPRUS



Prepared by the Digital Security Authority of Cyprus - NCCA
in collaboration with the "Working Group 4: EU and National
Legislations of NCC-CY"

