

A decorative graphic on the left side of the slide consists of several overlapping, curved bands in shades of purple, lavender, and green, sweeping upwards from the bottom left towards the top right.

A growing cybersecurity for products regulation - The Cyber Resilience Act

An ambitious and complex regulation

23/04/24 | Paul Chopineau & Ayoub Kara-Ali

The Cyber Resilience Act: an **ambitious regulation** ensuring the **security of EU citizens**

PROBLEM

Low levels of cybersecurity of products with digital elements.



SOLUTION

Policy intervention at EU level targeting the cybersecurity of products with digital elements.



ACTION(s)

Realization of studies focusing on the cybersecurity of digital products

OUTCOME

Proposal for a legislation defining the obligations of manufacturers, importers and distributors of products containing digital elements marketed in the EU that must bear the **CE mark across all sectors**.

An **evidence-based** assessment to make a **robust** legislation

We reach out to **every category of stakeholders** in the field

National competent authorities | EU bodies and agencies | HW manufacturers and SW developers | Trade associations | Consumer organizations | Researchers and academia | Cybersecurity industry professionals | EU citizens

We worked with best-in-class players



24 Interviews &
1 Targeted survey

2 Focus Groups
with **18** selected stakeholders

1 Open public consultation:
167 Answers over 2 months

2 Workshops :
More than **100** attendees each

List of relevant Products: **products with digital elements**



"A 'product with digital elements' means any **software** or **hardware** product and its remote data processing solutions, including software or hardware components to be placed on the market separately." (*Article 3*)



The CRA differentiates and details two types of product :
it designate '**products with digital elements**' and '**critical products with digital elements**'.



Consumer products



Smart cities



Industrial Control Systems



Firewalls



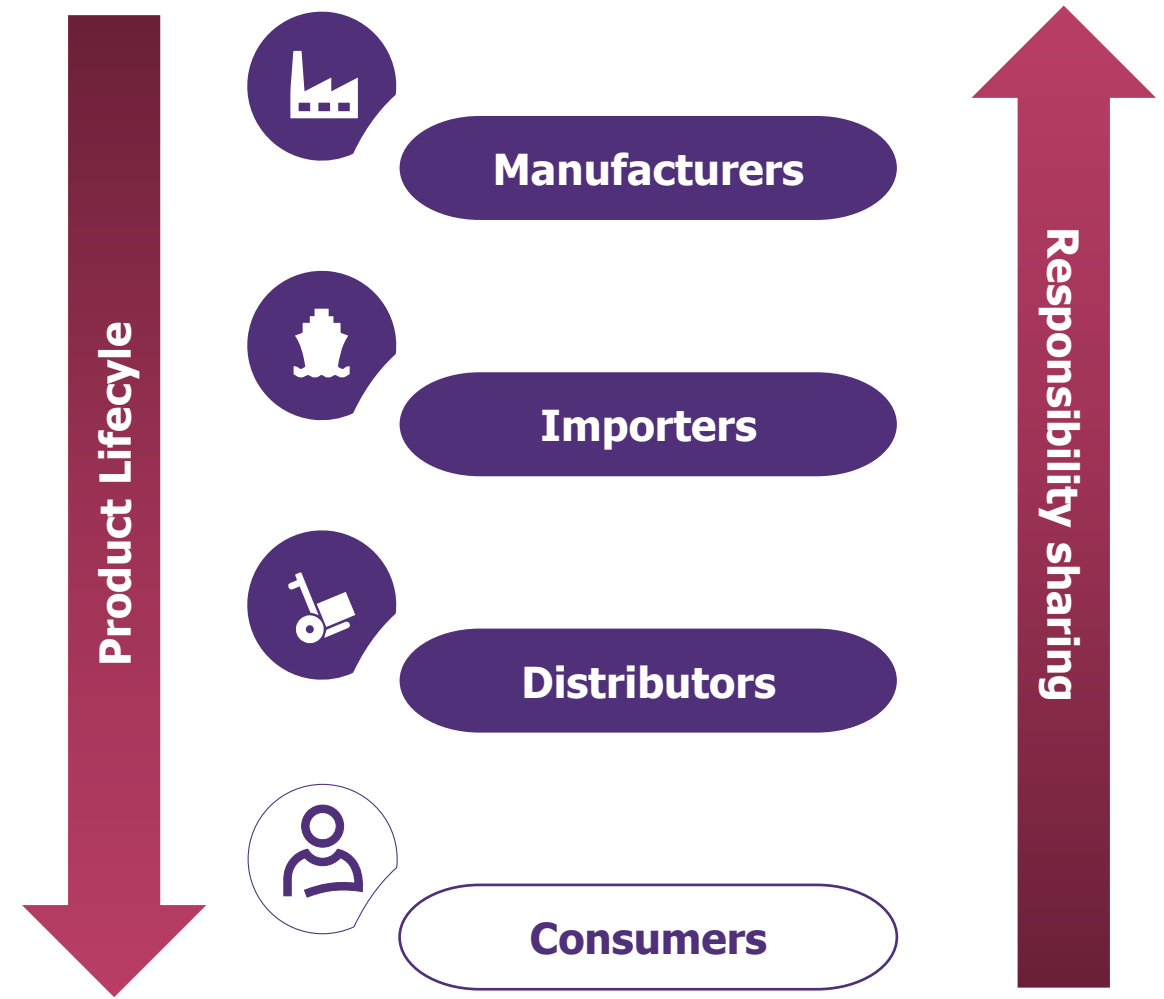
Software

Do you identify products on your scope?

Actors concerned by the CRA: everyone involved in the **product life cycle**

The Cyber Resilience Act involves the entire product **lifecycle**, from **development** by the manufacturer to **purchase** by the consumer

The first three stakeholders are subject to the act, which aims to **protect** the end **consumer**



Competent **Authorities** and **sanctions** mechanism

Like **GDPR**, each Member State shall determine the **penalties** applicable to infringements of this Regulation.



National legislator & market surveillance authorities



Noncompliance with the **essential cybersecurity requirements**

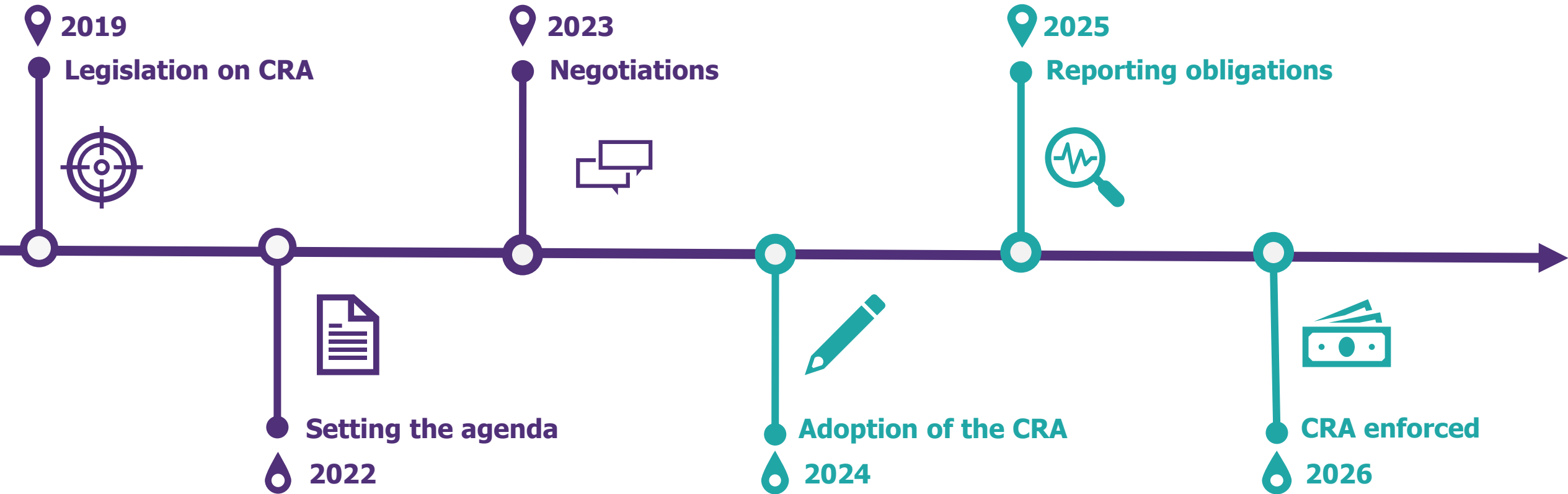
Administrative fines of up to **15 million €** or up to **2.5 % of the total worldwide annual turnover** for the preceding financial year.

Noncompliance with any **other obligations under this Regulation**



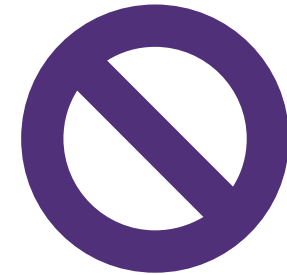
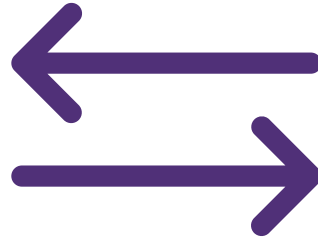
Administrative fines of up to **10 million €** or, if the offender is an undertaking, up to **2 % of its total worldwide annual turnover** for the preceding financial year.

The Cyber Resilience Act timeline: **almost 10 years** from identification to enforcement



2026: Obligation to comply with CRA cybersecurity requirements!

Interactions with the Cyber Resilience Act: thoughtful interconnections



The CRA is made for **interoperability**... And has **presumptions of conformity** ... but **not applicable to all sectors**

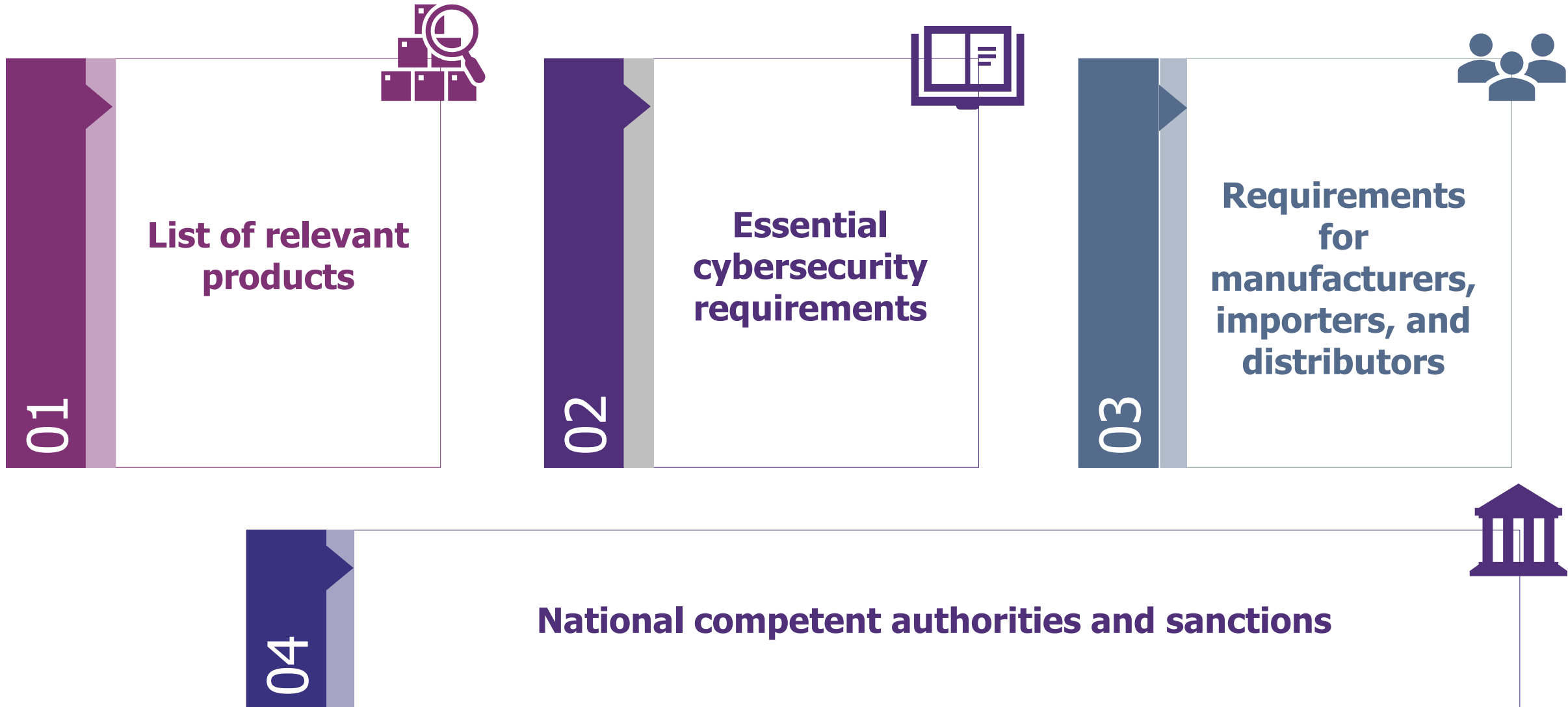
The CRA provides an EU-wide harmonized certification schema based on the regulatory framework

The digital components covered by these regulations satisfy those of the CRA

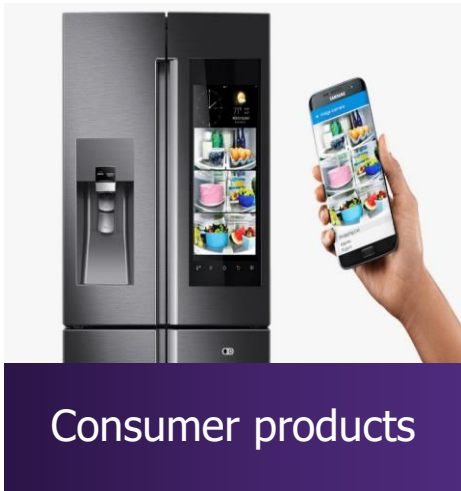
Some sectors are already covered by existing rules and are therefore not affected by the CRA



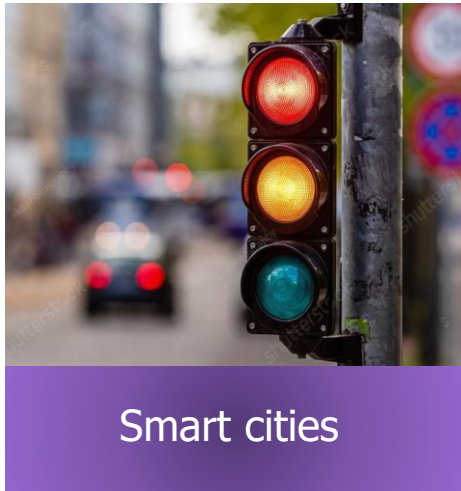
The Cyber Resilience Act's : a **complete coverage**



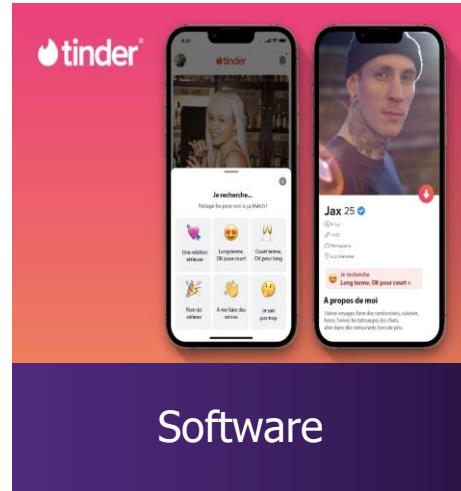
Products under the Cyber Resilience Act legislation's need assessments



Consumer products



Smart cities



Software



Self assessment



Industrial Control Systems



Firewalls



Third-party assessment



Critical products under the Cyber Resilience Act legislation's need **third party assessments**

Security products

From IAM to SIEM

Network systems

*Routers
Monitoring*

Hardware

TPM, CPUs & ASIC

Essential software

*Browsers, operating
systems and
hypervisors*

Infrastructure tooling

*Patch managers,
hypervisors*

Industrial Control Systems

From PLC to SCADA

Cybersecurity requirements for product with digital elements are built on 3 pillars

PRODUCT SECURITY REQUIREMENTS

- 01 Be designed, developed and manufactured in such a way as to guarantee an appropriate level of cybersecurity.
- 02 Be delivered without any known exploitable vulnerabilities.

USER NOTICE

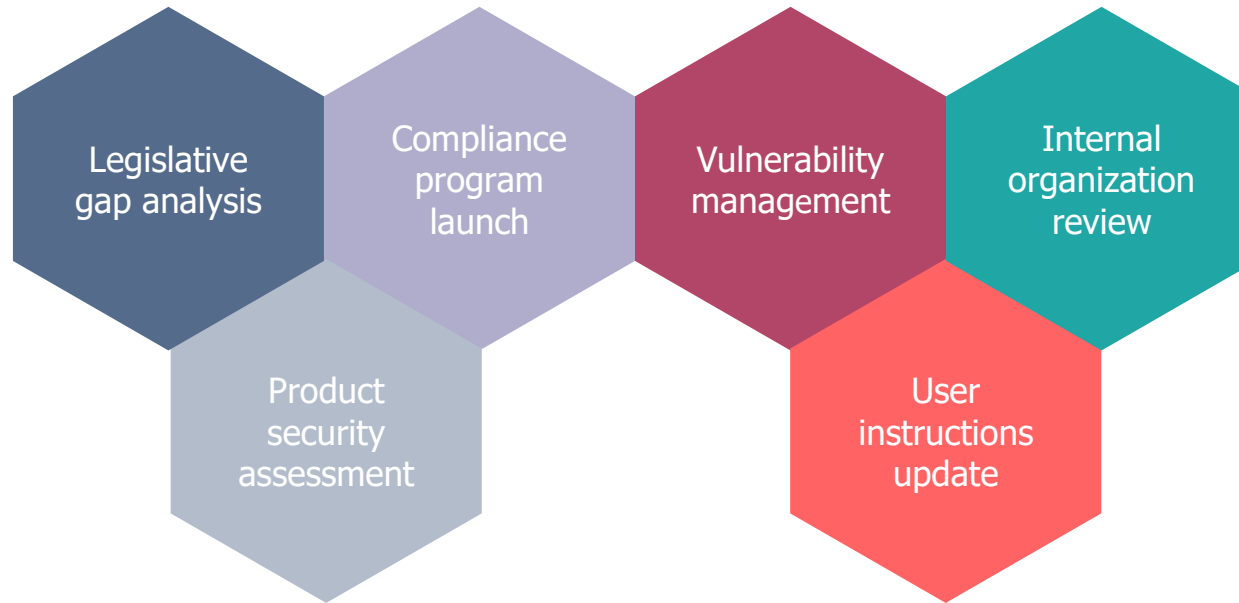
- 01 Be accompanied by documentation to ensure its safe use from commissioning to end of life.

VULNERABILITY MANAGEMENT REQUIREMENTS

- 01 Identify and document vulnerabilities and components contained in the product.
- 02 Be submissive regular and effective security tests and examinations.
- 03 Implement and enforce a vulnerability disclosure policy.

All requirements are available in the CRA Appendix.

Compliance: The Cyber Resilience Act **checklist**



Organizational framework

- / Security policies
- / Training and awareness
- / Access management



Product Security Framework

- / Data encryption
- / Strong authentication
- / Data integrity



Vulnerability Management

- / Continuous monitoring
- / Patch management
- / Management of known vulnerabilities

APPENDICES

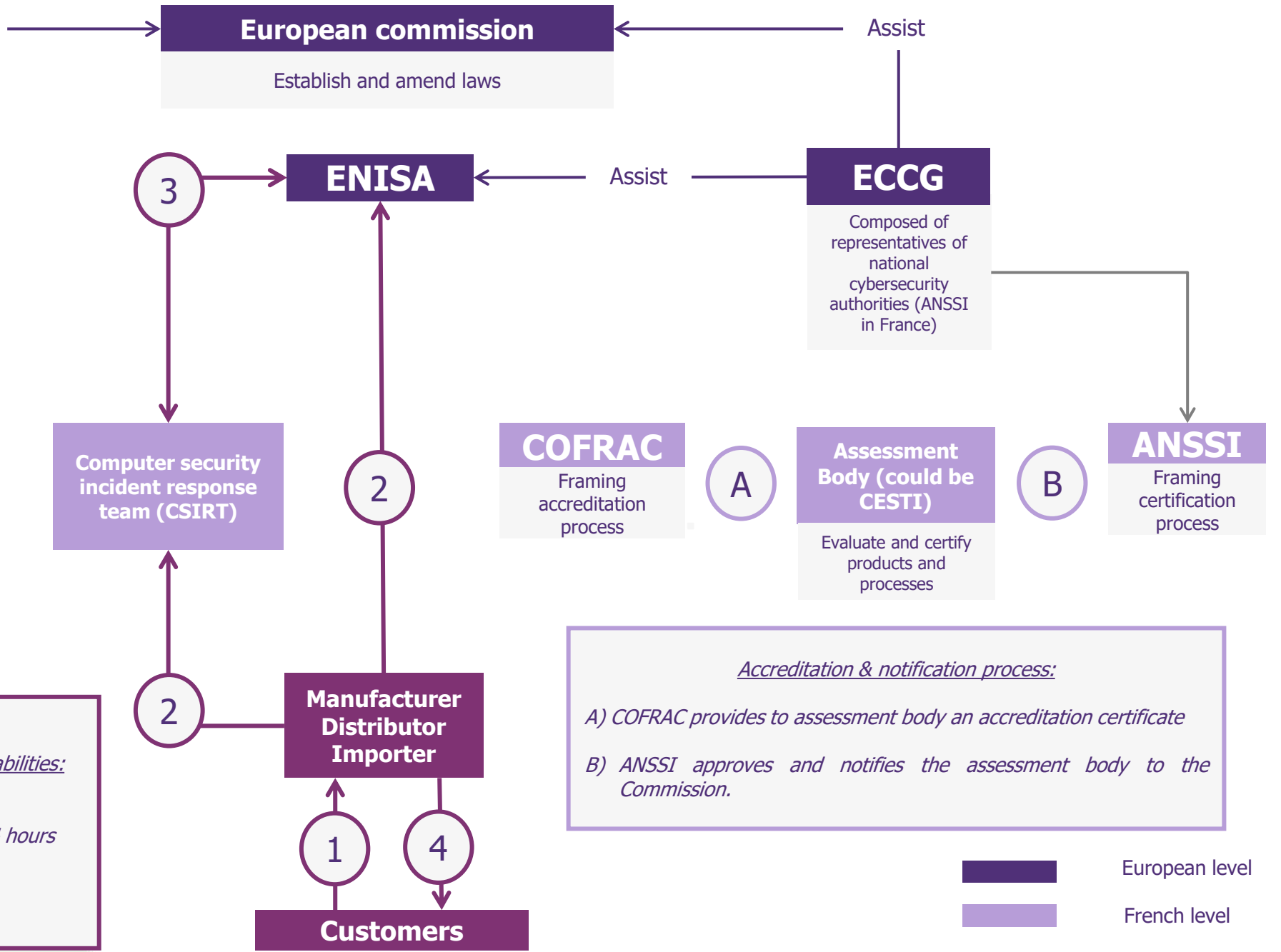
Guarantee uniform application of the legislation within the single market

AdCos
Composed of representatives of national market surveillance

General Directorate for Competition, Consumer Affairs and Fraud Control (DGCCRF)
Ensures market surveillance : Checks compliance with traffic regulations (such as CE marking)

Procedure for reporting incidents and vulnerabilities:

- 1) Reports vulnerabilities/incidents
- 2) Report incidents or vulnerabilities within 24 hours
- 3) Transfer notifications
- 4) Fix problems and make patches



- European level
- French level
- Economic actors

Links between the Cyber Resilience Act and standards covering digital components

Compatibility

*The digital components covered by these regulations satisfy those of the CRA and/or vice versa (**bilateral presumption of conformity**).*

- ✓ **High-risk** digital components (**as defined by the IA Act**) covered by the **IA Act**. [\(Link\)](#)
- ✓ **RED Directive** 2014/53/EU supplemented by Delegated Regulation (EU) 2022/30, which applies to all **radio equipment**. [\(Link\)](#)

It then remains to **demonstrate compliance** with the CRA assessment modules or a harmonized certification scheme. However, **if** the component is **identified as Class II**, whatever the standard in question, it **will have to** satisfy one of the **CRA assessment modules** (B+C or H).

*Digital components meeting the requirements of the CRA can meet the requirements of the following regulations (**unilateral presumption of conformity**)*

- ✓ Proposal for a regulation **on machinery and related products**. [\(Link\)](#)

Special case of the Cybersecurity Act

Players who have already started procedures with notified bodies may well continue their process, since these attestations of conformity remain valid 42 months after the promulgation of the CRA. Manufacturers should check with compliance bodies to see if any readjustments are necessary.

Incompatibilities


Manufacturers should check with compliance bodies to see if any readjustments are necessary.

- ✗ Regulation (EU) 2017/745 [**medical devices** for human use and accessories for such devices]. [\(Link\)](#)
- ✗ Regulation (EU) 2017/746 [in vitro **diagnostic medical devices** for human use and accessories for such devices]. [\(Link\)](#)
- ✗ Products with digital components that have been certified in accordance with Regulation (EU) 2018/1139 [uniform high level of **civil aviation** security]. [\(Link\)](#)
- ✗ Products to which Regulation (EU) 2019/2144 [on type-approval requirements for **motor vehicles** and their trailers, and for systems, components and separate technical units intended for such vehicles] applies. [\(Link\)](#)

Paul CHOPINEAU
Manager

M +33 (0)7 62 37 10 72
Paul.chopineau@wavestone.com

wavestone.com

 [Wavestone](#)