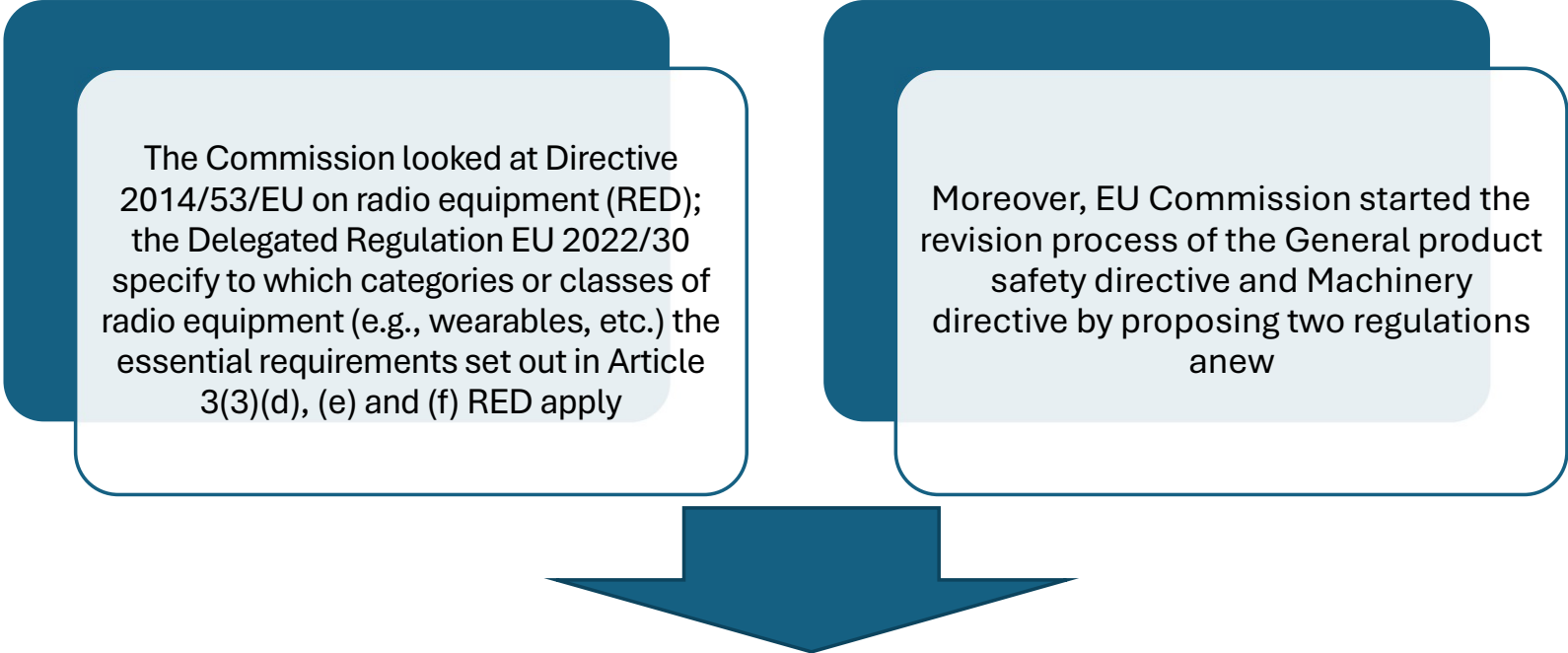


# Products (cyber)security: the EU Cyber Resilience Act

Pier Giorgio Chiara  
University of Bologna

# (Connected) products cybersecurity

With a view to addressing – in the short run – the overall level of cybersecurity of connected devices, the regulatory approach adopted by the Commission, from 2019 ca., revolved around the inclusion of minimum cybersecurity requirements in the directives and regulations of the ‘New Legislative Framework’ (NLF), that is, product safety legislation, through the adoption of delegated acts of the Commission or a revision of the legislative instrument in question

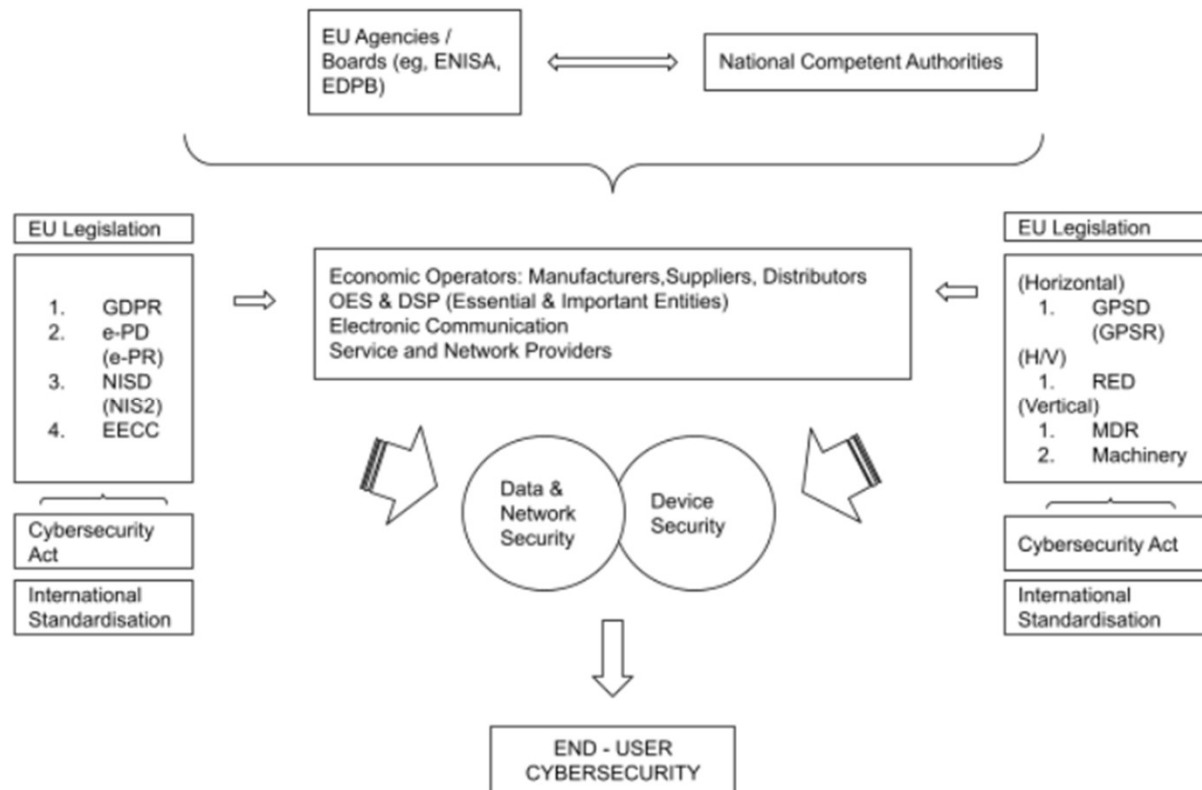


The Commission looked at Directive 2014/53/EU on radio equipment (RED); the Delegated Regulation EU 2022/30 specify to which categories or classes of radio equipment (e.g., wearables, etc.) the essential requirements set out in Article 3(3)(d), (e) and (f) RED apply

Moreover, EU Commission started the revision process of the General product safety directive and Machinery directive by proposing two regulations anew

The goal is to include in these legal acts cybersecurity-related essential requirements

# EU Cybersecurity regulatory landscape pre-CRA



# (Connected) products cybersecurity: the CRA

## ROOT CAUSES

- 1) A low level of cybersecurity of products with digital elements, due to widespread vulnerabilities and insufficient provision of security patches;
- 2) Lack of understanding and limited access to cybersecurity information by users of products with digital elements

## PROBLEM

**Hardware and software products are increasingly subject to cyber attacks, affecting an entire organisation or supply chain**

## LEGAL ISSUES

Most hardware and software products (especially 'non-embedded' software) are currently not (comprehensively) covered by any EU legislation with regard to their cybersecurity

## CYBER RESILIENCE ACT PROPOSAL

## GOALS

- i) ensure that manufacturers improve the security of products with digital elements since the design and development phase and throughout the whole life cycle;
- ii) ensure a coherent cybersecurity framework, facilitating compliance for hardware and software producers;
- iii) enhance the transparency of security properties of products with digital elements;
- iv) enable businesses and consumers to use products with digital elements securely

# (Connected) products cybersecurity: the CRA

## Scope

### applies to

products with digital elements made available on the market whose intended purpose or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network

### does not apply to

products with digital elements to which Regulation (EU) 2017/745; Regulation (EU) 2017/746; Regulation (EU) 2019/2144; Directive 2014/90/EU apply

products with digital elements that have been certified in accordance with Regulation (EU) 2018/1139

- products with digital elements developed exclusively for national security or military purposes or to products specifically designed to process classified information;
- spare parts to replace identical components in PDEs manufactured according to the same specifications

### application of the CRA may be limited or excluded

products with digital elements covered by other Union rules laying down requirements that address all or some of the risks covered by the essential requirements set out in Annex I

→ where such limitation or exclusion is consistent with the overall regulatory framework applying to those products

→ where the sectoral rules achieve the same level of protection as the one provided for by this Regulation

} Commission can adopt delegated acts specifying whether such limitation or exclusion is necessary, the concerned products and rules, as well as the scope of the limitation

# (Connected) products cybersecurity: the CRA

## Scope

applies to

**products with digital elements** made available on the market whose intended purpose or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network

any software or hardware product including its remote data processing solutions, and software or hardware components to be placed on the market separately (Art. 3(1))



**Hardware products** and components placed on the market separately, such as laptops, smart appliances, mobile phones, network equipment or CPUs



**Software products** and components placed on the market separately, such as operating systems, word processing, games or mobile apps



**Non-commercial projects, including open source** in so far as a project is not part of a commercial activity



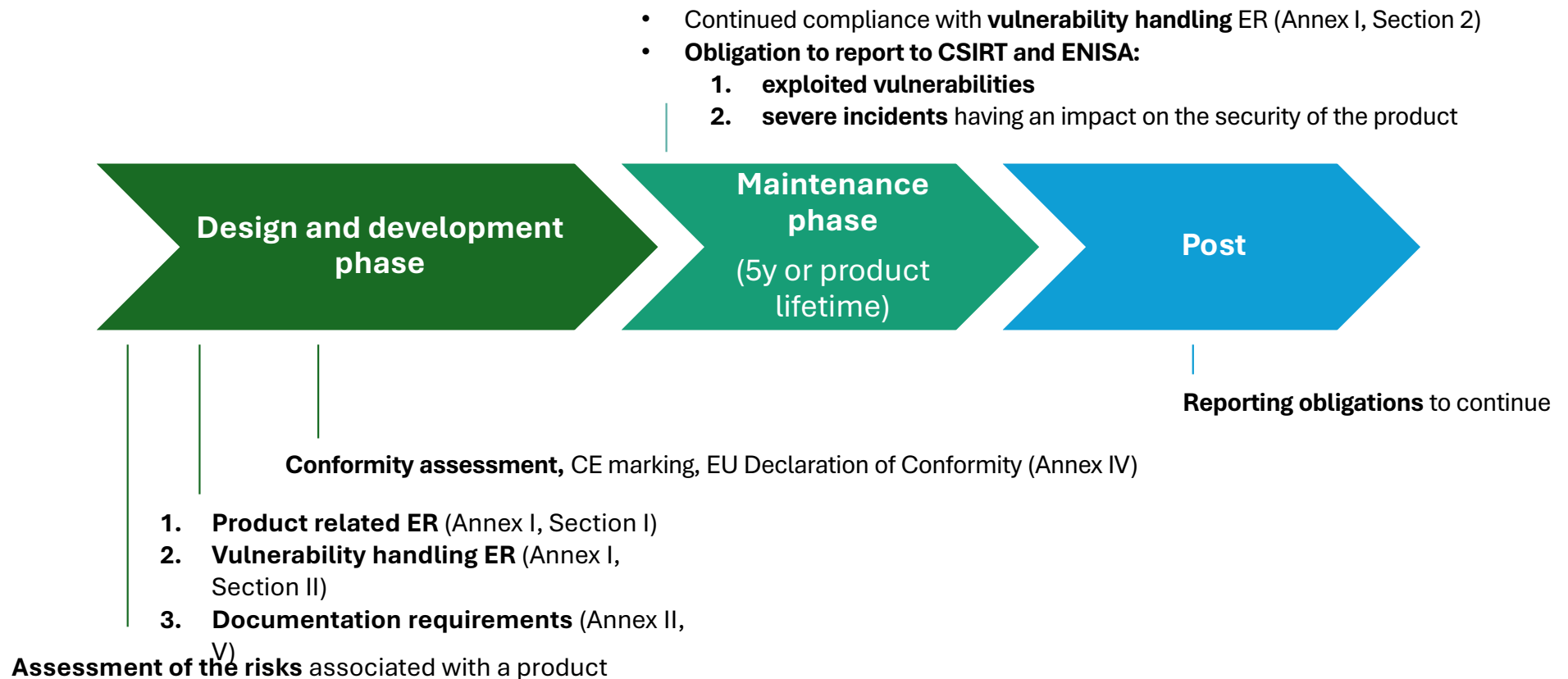
**Services, in particular cloud/Software-as-a-Service** – covered by NIS2



**Outright exclusion** (cars, medical and in-vitro devices, certified aeronautical equipment, marine equipment)

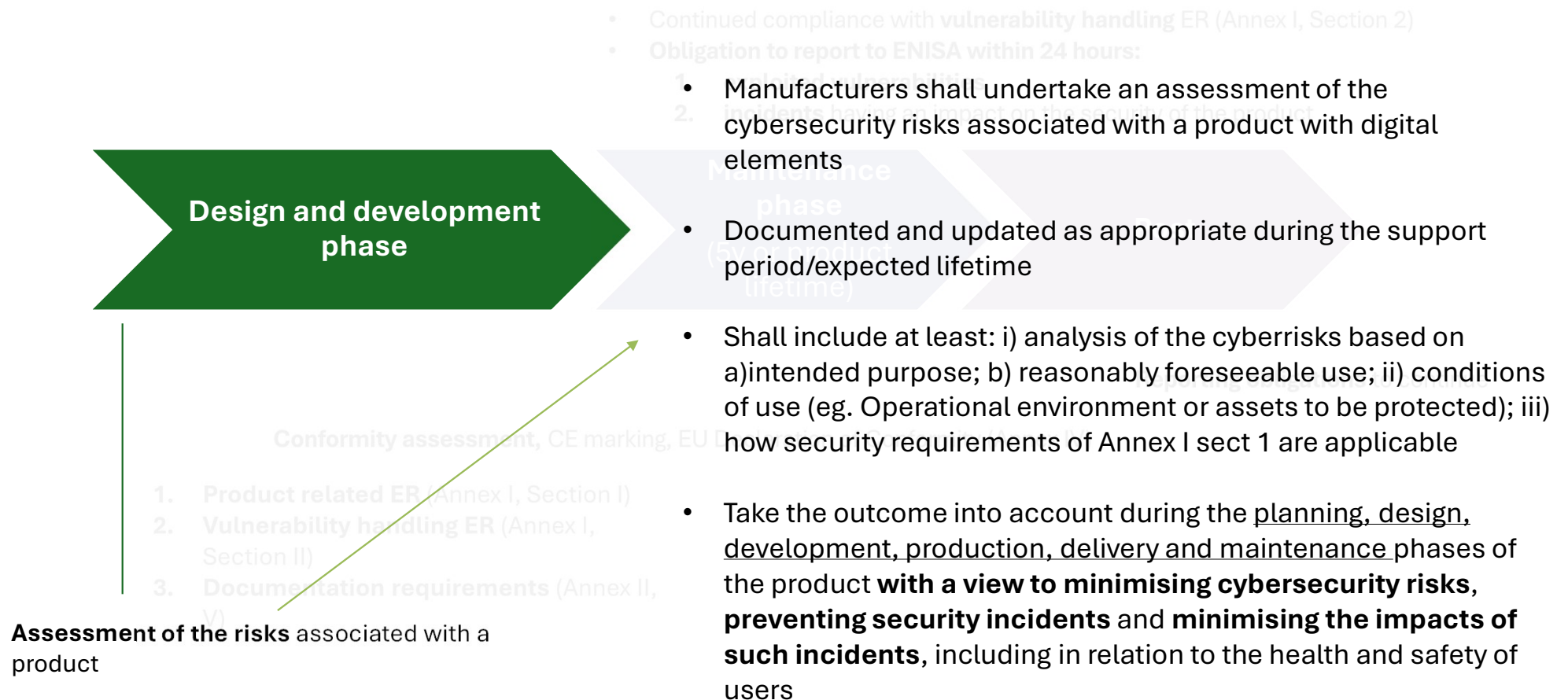
# (Connected) products cybersecurity: the CRA

## Obligations of manufacturers



# (Connected) products cybersecurity: the CRA

## Obligations of manufacturers





# (Connected) products cybersecurity: the CRA

## Obligations of manufacturers



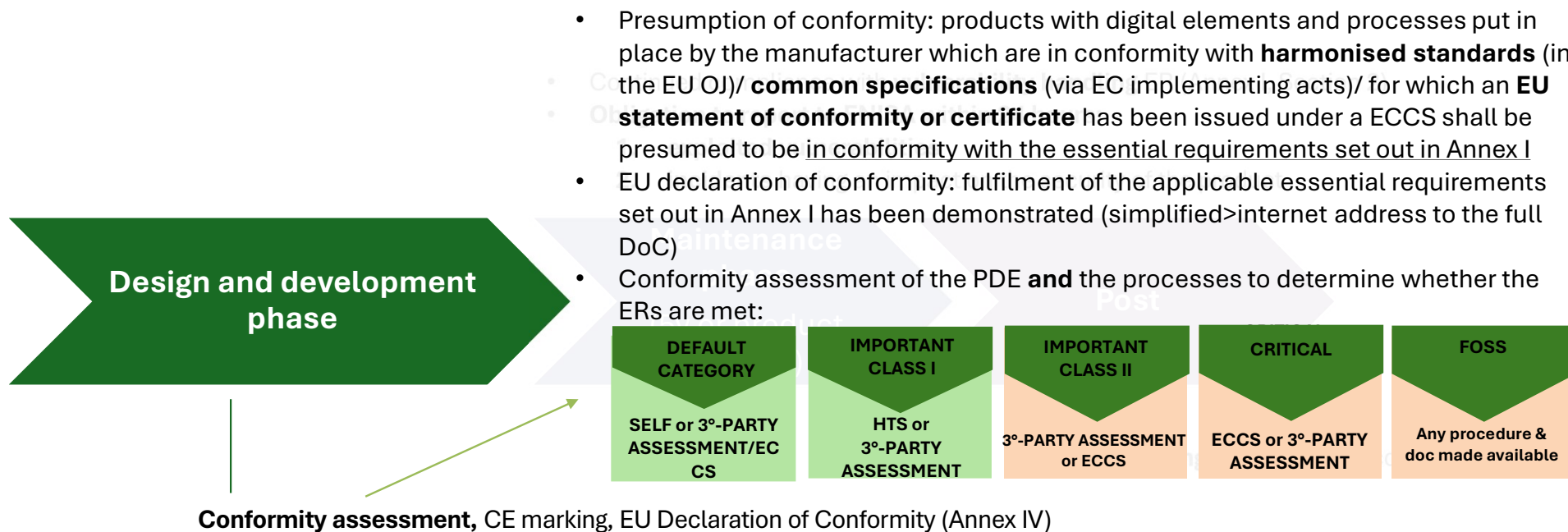
1. **Product-related ER** (Annex I, Section I)
2. **Vulnerability handling ER** (Annex I, Section II)
3. **Documentation requirements** (Annex II, V)

Assessment of the risks associated with a product (Annex III)

- **Product-related ER:**
  1. Designed, developed and produced to ensure an appropriate level of cybersecurity based on the risks;
  2. On the basis of the **risk assessment**: shall be made available without known exploitable vulnerabilities; made available with a secure by default configuration; ensure that vulnerabilities can be addressed through security updates; shall ensure protection from unauthorised access by appropriate control mechanisms; shall protect the confidentiality of processed personal or other data by means of state-of-the-art encryption, etc.
- **Vulnerability handling ER:**
  1. Identification and documentation of vulnerabilities and components contained in the product, including by drawing up a software bill of materials (SBOM) in a commonly used and machine-readable format covering at the very least the top-level dependencies of the product
  2. Mitigation of vulnerabilities without delay, including by providing security updates
  3. The application of effective and regular tests and reviews of the security of the product
  4. The public disclosure of information about fixed vulnerabilities, once a security update has been made available, etc.
- **Documentation requirements** regarding handling vulnerabilities and information provided by third parties:
  - Technical documentation to be drawn up by the manufacturer before the product is placed on the market and to be kept at the disposal of the market surveillance authorities for ten years after the product has been placed on the market (cfr. Art. 10, 23 and Annex V)
  - Information and instruction to the user (Annex II)
  - Shall include the risk assessment

# (Connected) products cybersecurity: the CRA

## Obligations of manufacturers



- Presumption of conformity: products with digital elements and processes put in place by the manufacturer which are in conformity with **harmonised standards** (in the EU OJ)/ **common specifications** (via EC implementing acts)/ for which an **EU statement of conformity or certificate** has been issued under a ECCS shall be presumed to be in conformity with the essential requirements set out in Annex I
- EU declaration of conformity: fulfilment of the applicable essential requirements set out in Annex I has been demonstrated (simplified>internet address to the full DoC)
- Conformity assessment of the PDE **and** the processes to determine whether the ERs are met:

1. Product related ER (Annex I, Section I)
2. Vulnerability handling EF (Annex I, Section II)
3. Documentation requirements (Annex II, V)



- CE marking
- Chapter IV: Member States designate a notifying authority responsible for setting up and carrying out the necessary procedures for the assessment and notification of conformity assessment bodies and monitoring of notified bodies

Assessment of the risks associated with a product

# (Connected) products cybersecurity: the CRA

## Obligations of manufacturers

Manufacturers inform **users** of the product about the incident/vulnerability and about corrective measures to be deployed to mitigate the impact of the incident  
CSIRTs may provide such info to users if manufacturer fail to provide said info in a timely manner

- 1) early warning: 24hours
- 2) vulnerability/incident notification: 72hours
- 3) CSIRTs may request manufacturers intermediate report
- 4) Final report: 14 days after a corrective/mitigating measure is available and 1 month after incident notification

1. **Product related ER** (Annex I, Section I)
2. **Vulnerability handling ER** (Annex I, Section II)
3. **Documentation requirements** (Annex II, V)

Assessment of the risks associated with a product

- Continued compliance with **vulnerability handling ER** (Annex I, Section 2)
- **Obligation to report to CSIRT and ENISA** via single reporting platform:
  1. **exploited vulnerabilities**
  2. **Severe incidents** having an impact on the security of the product

**Maintenance phase**  
(5y or product lifetime)

Manufacturers report the vulnerability to **the person or entity manufacturing or maintaining** the component (including open-source) affected by the vulnerability integrated in the product

If manufacturers 'fix' components' vulnerability, they have to share the fix to the entity responsible for the component

+ **Voluntary reporting:** manufacturers/other natural or legal persons may notify any vulnerability/incident to CSIRT or ENISA

# (Connected) products cybersecurity: the CRA

## Market Surveillance and Enforcement

National market surveillance authorities (MSAs)—designated by Member States—carry out market surveillance in that Member State

### COOPERATION

MSAs under the CRA shall *cooperate* with: ENISA (technical advice); **other MSAs** designated on the basis of other Union harmonisation legislation for other products; **national cybersecurity certification authorities** designated under the CSA and **DPAs**

- Joint activities between MSAs can be carried out with the aim of ensuring cybersecurity and protection of consumers
- MSAs may decide to conduct simultaneous coordinated control actions (“sweeps”) of particular products to check compliance with the CRA

### POWERS

If a product does not comply with the CRA, MSA shall without delay **require** the relevant operator to **take all appropriate corrective actions to bring the product into compliance** with those requirements, to **withdraw it from the market**, or to **recall it** within a reasonable period

### PENALTIES

MSs to set rules on penalties but: i) noncompliance with **Annex I ERs** and **Art. 10 and 11 obligations** administrative fines 15M EUR/2.5% total worldwide annual turnover; ii) noncompliance with any other obligations 10M/2%; and, iii) incorrect, incomplete or misleading information to notified bodies and MSAs 5M/1%