



Cyber Resilience Act

7th February 2023

*Maika FOHRENBACH
European Commission, DG CONNECT*

Main elements of the proposal

- ❖ **Cybersecurity rules** for the placing on the market of hardware and software
- ❖ Based on **New Legislative Framework** (well-established EU product-related legislative setting)
- ❖ **Obligations** for manufacturers, distributors and importers
- ❖ Cybersecurity **essential requirements** across the life cycle (5 years)
- ❖ Harmonised **standards** to follow
- ❖ **Conformity assessment** – differentiated by level of risk
- ❖ **Market surveillance and enforcement**

Scope

Products with digital elements:

- + **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
- ① The definition of “**products with digital elements**” also includes **remote data processing solutions**.

Not covered:

- ✗ **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** – *except “remote data processing solutions”*

Outright exclusions:

- ✗ **Certain products sufficiently regulated on cybersecurity** (cars, medical devices, *in vitro*, certified aeronautical equipment) under the new and old approach

Obligations of manufacturers

Assessment of the risks associated with a product

- (1) **Product-related** essential requirements (Annex I, Section 1)
- (2) **Vulnerability handling** essential requirements (Annex 1, Section 2)
- (3) **Technical file**, including **information and instructions** for use (Annex II + V)

Conformity assessment, CE marking, EU Declaration of Conformity (Annex IV)

Continued compliance with **vulnerability handling** essential requirements throughout the product life time (Annex I, Section 2)

Design and development phase

Maintenance phase
(5 years or across product lifetime, whichever is shorter)

Obligation to report to ENISA within 24 hours:

- (1) **exploited vulnerabilities**
- (2) **incidents** having an impact on the security of the product

Reporting obligations to continue

Standards & presumption of conformity

❖ Harmonised standards

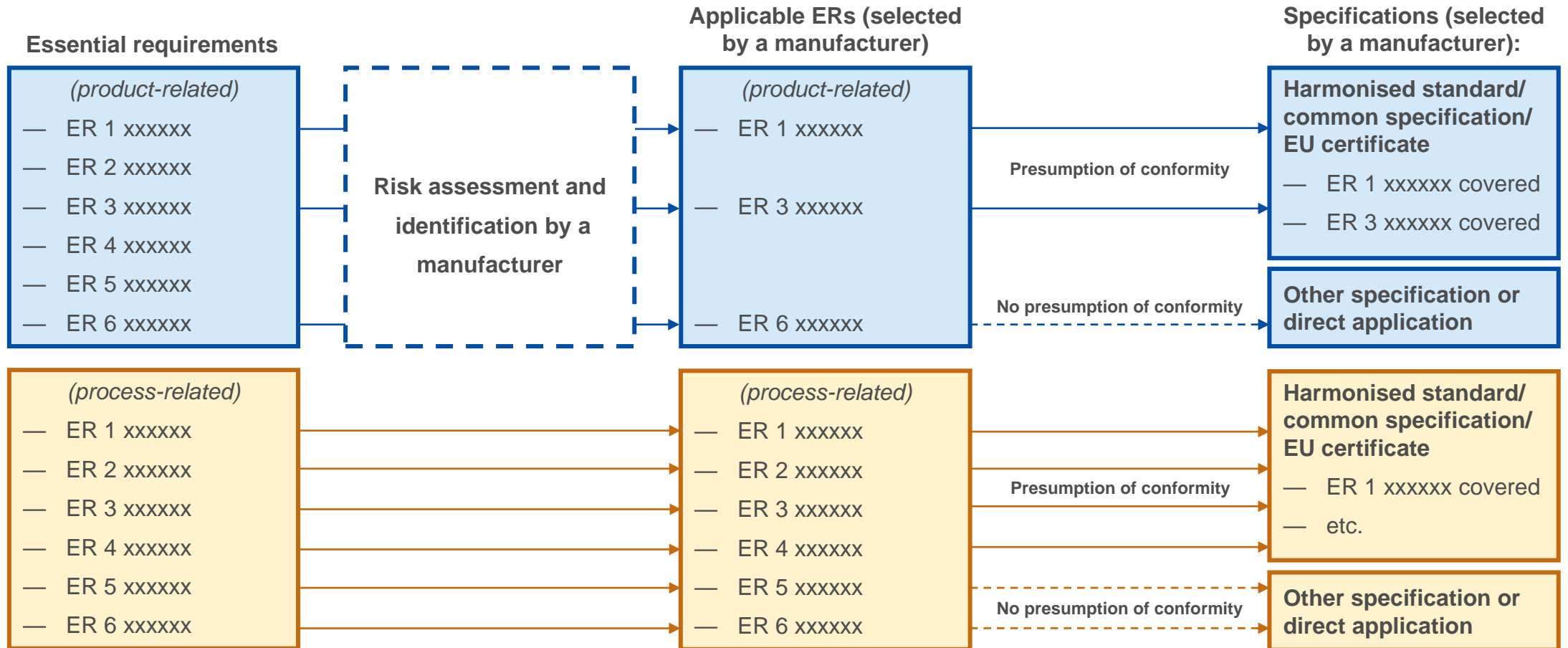
❖ Upon Commission request, to be developed by European Standardisation Organisations (ESOs)

❖ Preparatory work has started 

❖ EU cybersecurity **certification schemes**

❖ **Common specifications**

Identification of essential requirements



Tentative timeline

