

# SEC4YOU

Advanced IT-Audit Services

PUBLIC TLP:CLEAR

## Roadmap to Cyber Resilience Act (CRA)

Supporting teams to transform hardware and software offerings in CRA compliant products

Andreas Schuster | René Pfeiffer, January 2026, Version 1.4

# RESILIENCE

---

*resilience*, : The positive capacity of an organizational system or company to adapt and return to equilibrium after a crisis, failure or any kind of disruption, including: an outage, natural disasters, man-made disasters, terrorism, or similar (particularly IT systems, archives) [Wikipedia]

- RESILIENCE is often mentioned without definition: System resilience  $\neq$  organisational resilience
- RESILIENCE means:
  - to **continue with intended operations** when under attack
  - **not failing under load** or other disruptive influences
  - to **fail in a controlled fashion** (fail securely/safely)
  - to **contain the damage** of attacks / unintended actions

# Cyber Resilience Act (CRA) Summary

- Applicable for products with digital elements placed on the EU market
- Obligations for
  - Manufacturer
  - Authorized representatives
  - Importers
  - Distributors

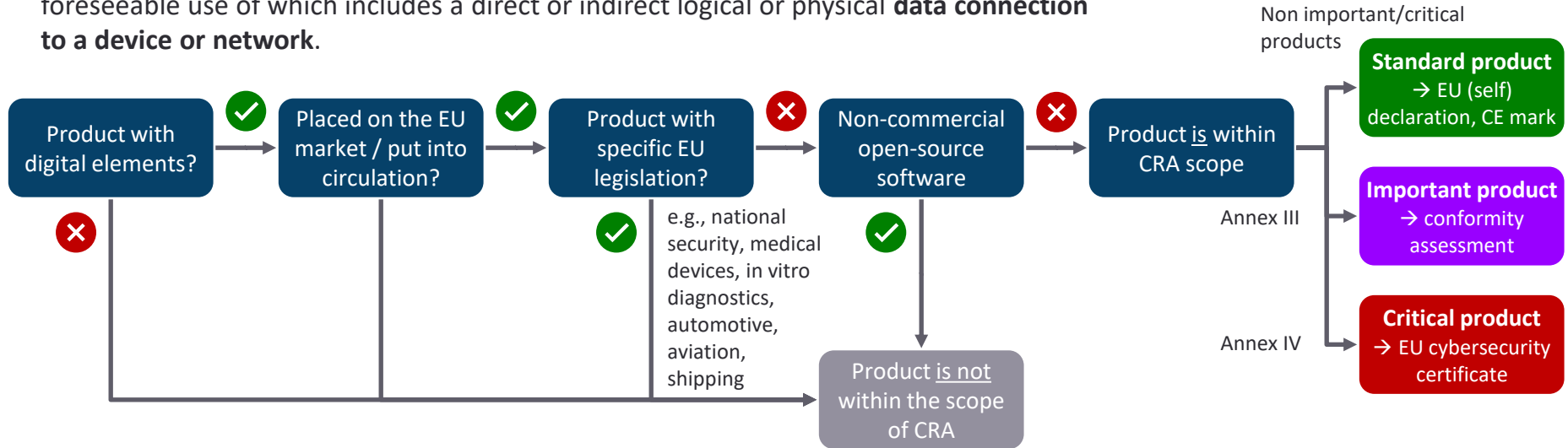
not considered in this roadmap



# Decision Tree Cyber Resilience Act (CRA)

CRA regulates „products with digital elements“...

A product including **software** and/or **hardware** that intended purpose or reasonably foreseeable use of which includes a direct or indirect logical or physical **data connection** to a device or network.



## Cyber Resilience Act (CRA) Summary

- Three product risk categories
  - **Standard products** including end user hardware/software and business hardware/software
  - **Important products** according to annex III e.g., IDM, password manager, malware protection, operating systems, baby monitoring, alarm systems and much more
  - **Critical products** according to annex IV e.g., hardware security devices, crypto processing, smart meter gateways, smartcards



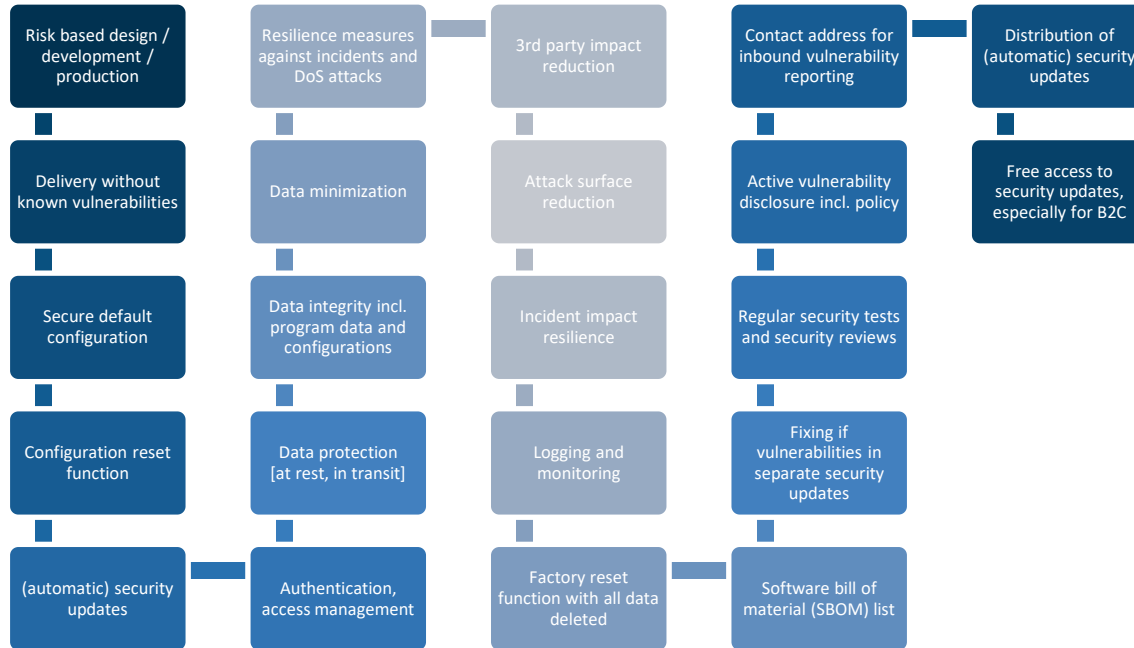
## Deadlines!

---

- In force since **December 10, 2024**
- **Government: June 11, 2026**, Chapter IV – Setup of notification authorities (per country)
- **Manufacturer: September 11, 2026**, Article 14 - Reporting obligations of manufacturers
- **Manufacturer: Fully applicable December 11, 2027**, focus on:
  - Secure by Design in Secure Development Lifecycle (SDLC)
  - Annex I - Essential Cybersecurity Requirements, incl. cybersec requirements and vulnerability management
  - Annex II – Information and Instructions to the User, incl. software bill of materials (SBOM)
  - EU declaration of conformity + CE marking



# Essential Cybersecurity Requirements

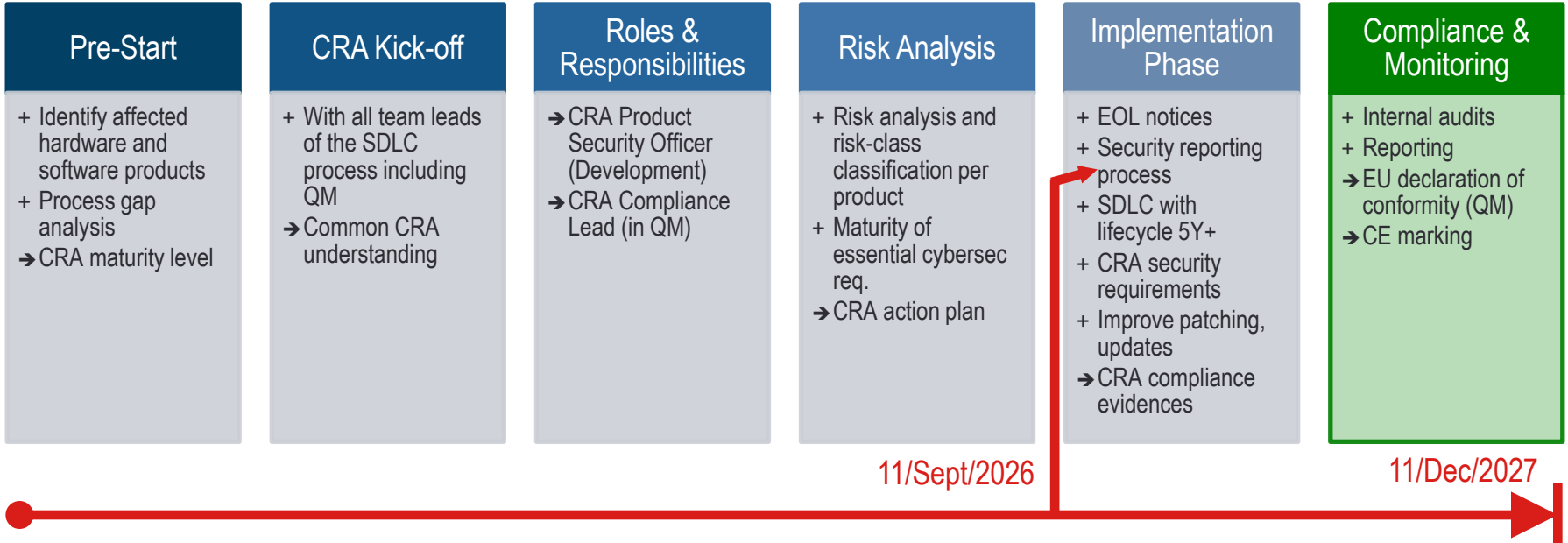


# Software Development Lifecycle (SDLC)

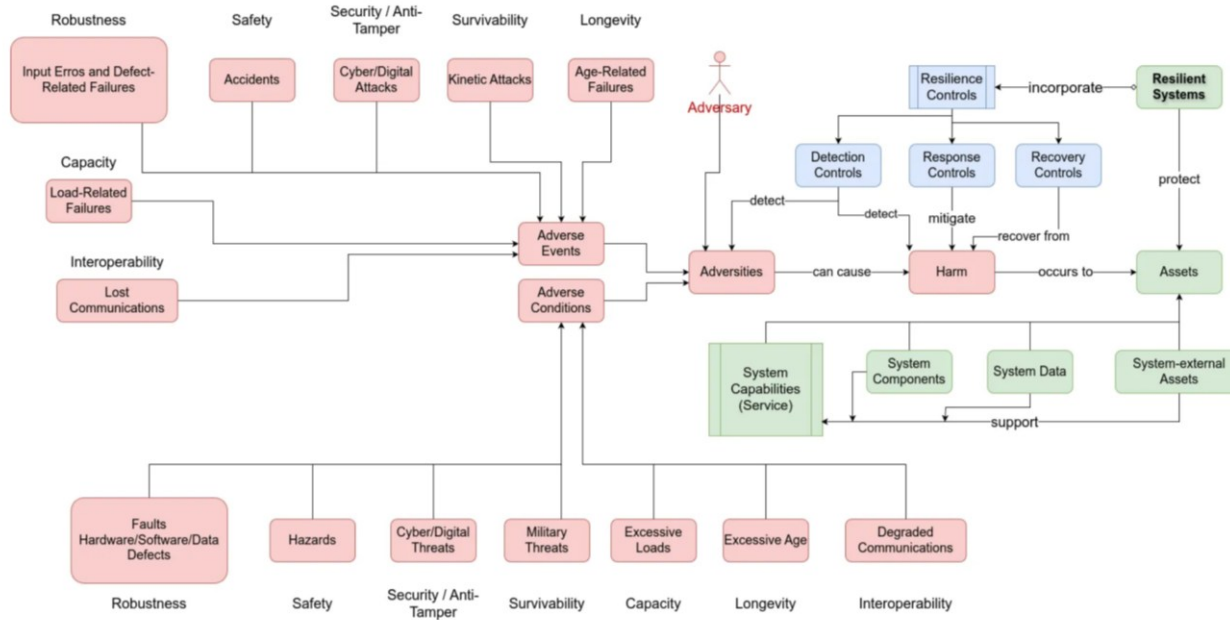
- Many of the essential cybersecurity requirements can be addressed by implementing a SDLC in your development team.
- A full SDLC is available in the SEC4YOU Secure Coding Manual designed for product development teams:  
<https://www.sec4you.com/en/produkt/template-secure-coding-manual>



# Simplified Roadmap to Cyber Resilience (Manufacturer only)



# How to implement resilience?



# Steckbrief „Cyber Resilience Act (CRA)“

## Kurzfassung

Der Cyber Resilience Act (CRA) ist eine am 10. Dezember 2024 in Kraft getretene EU-Verordnung (EU 2024/2847), die ab dem 11. Dezember 2027 die Cybersicherheit für alle Produkte mit digitalen Elementen – also Hardware, Software und dazugehörige Remote-Dienste – verbindlich regelt.

Fristen: (1) Meldepflicht Schwachstellen: 11.09.2026, (2) Einhaltung der CRA-Vorgaben für neue Produkte: 11.12.2027

## Betroffen

- Hersteller
  - Importeure
  - Distributoren
  - Software-Entwickler → gelten als Hersteller
- Keine Einschränkung auf die Unternehmensgröße!*

## Produkte

Drei Risikoklassen:

**Standardprodukte** → Selbstbewertung

**Wichtige Produkte** wie Betriebssysteme, Sicherheitssysteme, u.a. auch Babyüberwachung  
→ externe Prüfung oder Konformitätsbewertung

**Kritische Produkte** → Cybersicherheitszertifizierung

## Anforderungen (vereinfacht)

- Risikobasiertes Cybersicherheitsniveau\* im Design, Entwicklung und Produktion
  - Auslieferung ohne bekannte, ausnutzbare Schwachstellen + SBOM Liste [Anh. I, 2. (1)]
  - Sichere Standardkonfiguration und vollständige Rücksetzbarkeit
  - Updatefähigkeit + kostenfreie Sicherheitsupdates für mind. 5 Jahre [Art. 10 (6)]
  - Zugriffsschutz / Authentifizierung
  - Vertraulichkeit der verarbeiteten Daten inkl. personenbezogenen Daten
  - Datenminimierung, Angriffsflächenminimierung, Auswirkungsminimierung auf 3rd Party
  - Protokollierung oder Überwachung von internen Vorgängen
  - Prozess zur Handhabung von Schwachstellen inkl. Offenlegung und Sicherheitsupdates
- \*) erfordert Secure Design, Secure Coding und einen SDLC [Anh. I, 1. (1)]*



# Questions?

---



[rene.pfeiffer@sec4you.com](mailto:rene.pfeiffer@sec4you.com)  
<https://sec4you.com>  
Tel.: +43 2262 72857

