IAPP Europe **Data Protection Congress 2025**

Training 17-18 November

Workshops 18 November

Conference 19-20 November

BRUSSELS

#DPC25

Cyber Resilience Act sliced and diced

19 November 2025

Speakers

Maria Aholainen, CIPP/E, Counsel, Hannes Snellman

Kira Ahveninen-Kuha, Global Lead Digital Counsel, ABB

Jussi Leppälä, AIGP, CIPP/E, CIPT, CIPM, FIP, CISSP, Valmet

Agenda

I. Welcome and Introductions
II. CRA in a nutshell
III. Key Commercial Questions
IV. Standardization
V. Interplay with other EU laws

Key take-aways

I. Key commercial questions that arise from CRA
II. How to split the CRA into categories of requirements and their stakeholder base
III. Where and where not to refer to standardization and IEC 62443 on the CRA journey
IV. How does the CRA intersect with other cybersecurity and data laws

CRA – cybersecurity as a permanent property of the product

What is PDE?

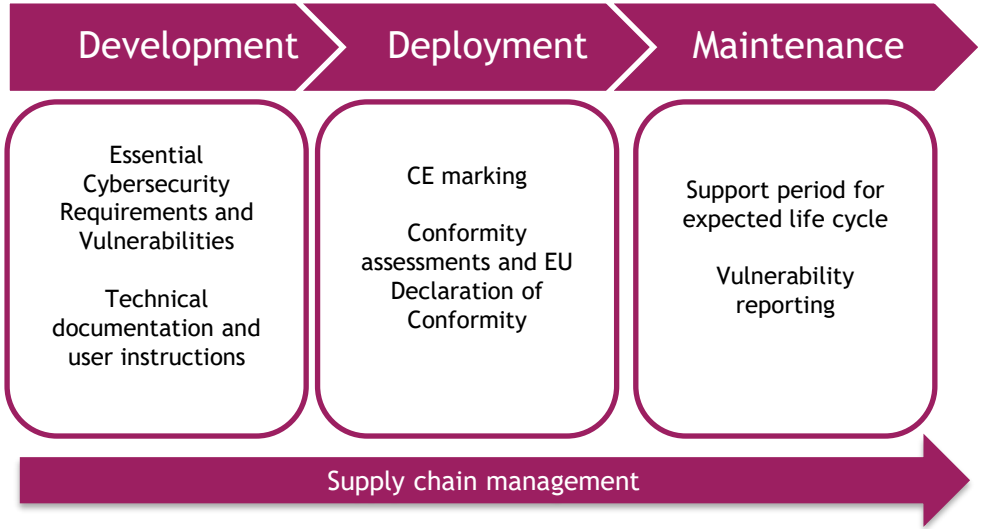
Products with digital elements (PDE)

- software or hardware product
- remote data processing solutions

Outside the scope

- Medical devices
- Motor vehicles
- Civil aviation
- Products exclusively for national security or defence purposes
- Open-source software that is not commercially distributed

Manufacturer's key obligations



Product classification

90 % of products

Category	Default category	Important products		Critical products
		Class I	Class II	
Conformance	*Self-assessment*	*Harmonised standard or third-party assessment*	*Third-party assessment*	*EUCC certification*
Criteria	*N/A*	*Assessment: core function & intended use*		
Example	*All products NOT classified as important or critical*	*Password managers, operating systems, microcontrollers and processors with safety-functions*	*Industrial firewalls, intrusion detection, tamper-resistant microcontrollers and processors for industrial control*	*Smartcards, smart meter gateways, any product leading to critical dependency of essential infrastructure*

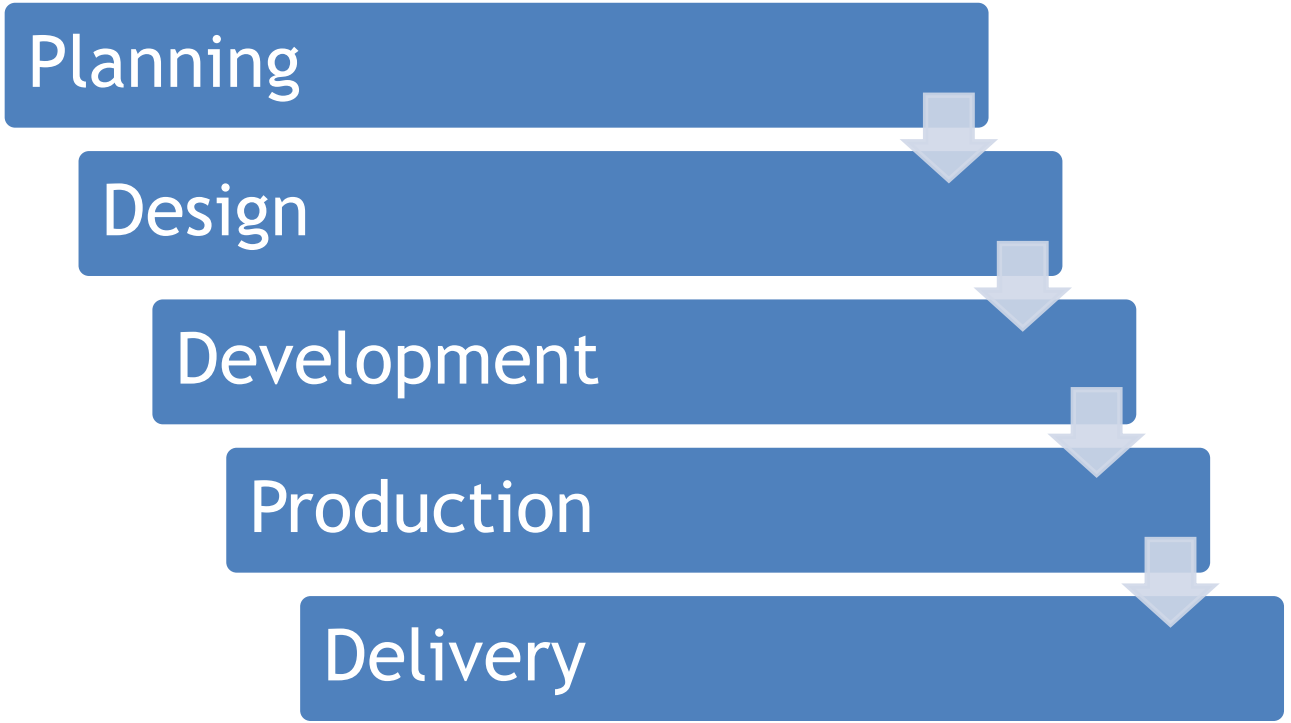
Role of standardization

- Certification strategy for Important Class I
- Can be a good benchmark
- Standards are in themselves of voluntary application
- Harmonized Standards published in the Official Journal of the European Union provide a ***presumption of conformity*** with the legislative requirements they aim to cover
- May also cover non-regulated issues
- Horizontal and Vertical standards for EU CRA
- CRA for OT = EN IEC-62443?

Risk Assessment and Essential Cybersecurity Requirements

PDEs shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks. => Secure Development Lifecycle

Lifecycle phases and risk assessment

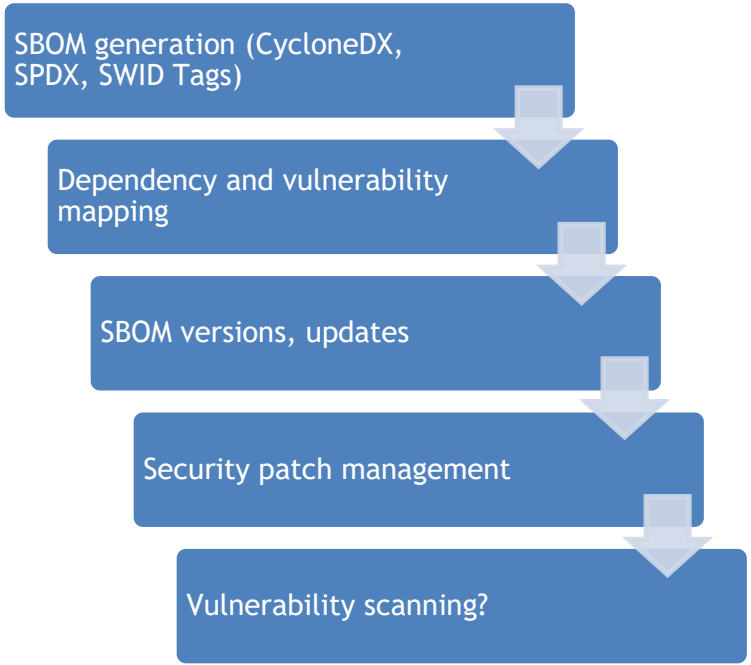


Essential Cybersecurity Requirements

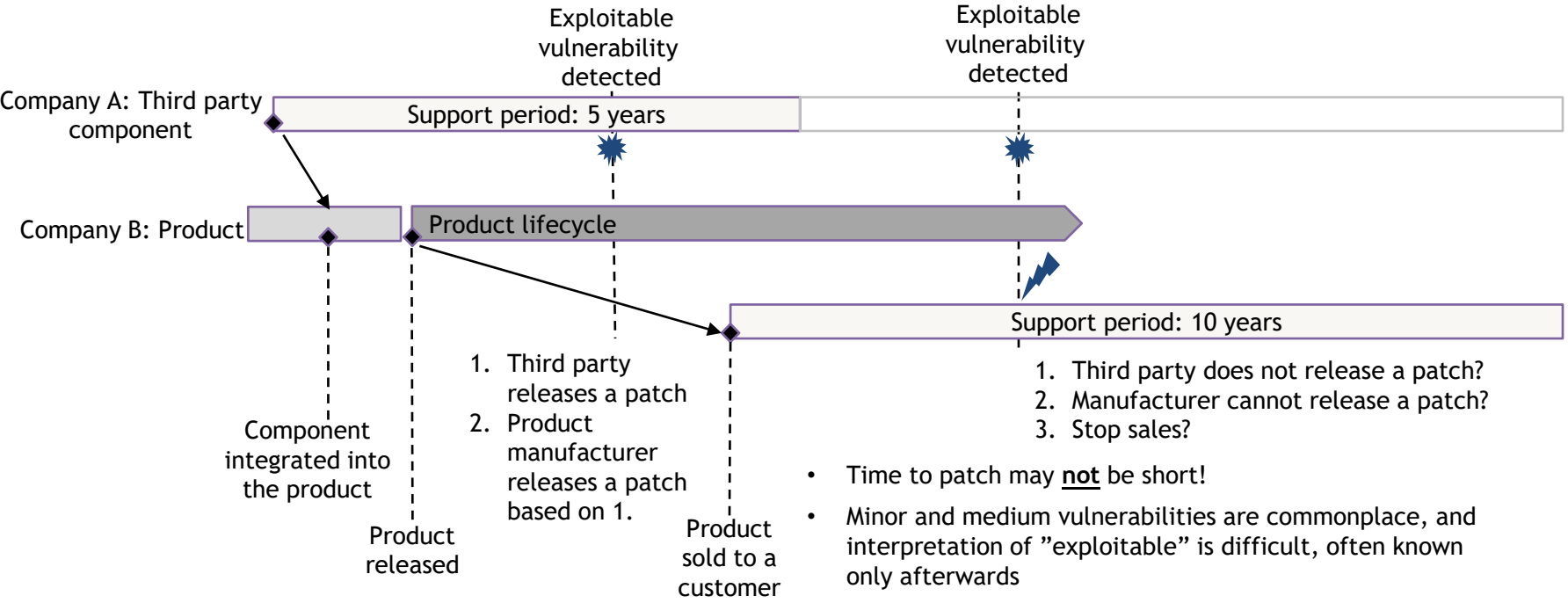
- Be made available on the market without known exploitable vulnerabilities
- Secure by default configuration .. including the possibility to reset the product to its original state
- Security updates..
- Access management
- Protect the confidentiality..
- Protect the integrity..
- Data minimization (GDPR)
- Protect the availability
- Minimize negative impact on others
- Minimize attack surfaces
- Reduce the impact of incidents
- Provide security related information (Data Act)
- Possibility to remove all data and settings

Technical documentation and Software Bill of Materials

- Requirement for vulnerability management and as a part of technical documentation for authorities. CRA does not require sharing SBOM with the user.
- Possibility for implementing acts specifying “the format and elements” of SBOMs



Third Party Components and Business dependencies

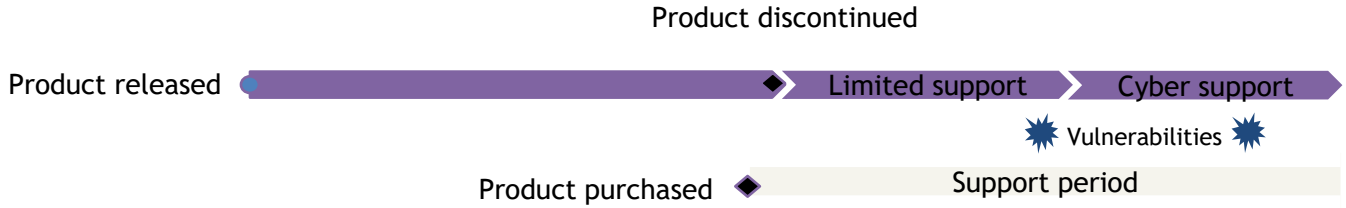


- Time to patch may **not** be short!
- Minor and medium vulnerabilities are commonplace, and interpretation of ”exploitable” is difficult, often known only afterwards

Free security upgrades during support period

Support period: Period to remediate security vulnerabilities with **free updates**

- Reflects the length of time during which a product is expected to be in use at a customer
- Starts with purchase of product by customer (not with the product release)
- An upgrade sold to the customer may restart the clock on the support period!



As a result, manufacturer may potentially spend significant effort “for free” after a product is initially sold

Vulnerability and Incident Management

- Two authority (ENISA and CSIRTs) reporting requirements:
  - actively exploited vulnerabilities
  - severe incidents
  - both with 24 h, 72 h, and final reports
- Vulnerability disclosure process

Actively exploited vulnerabilities – notification timeline

Early warning

- Within 24 hours
- Must indicate Member States where the product has been made available

Vulnerability notification

- Within 72 hours
- Vulnerability and mitigating measures

Final report

- No later than 14 days
- Information on vulnerability, malicious actor that has exploited it, details about the corrective measures

Severe incidents – notification timeline

Early warning

- Within 24 hours
- Must indicate the Member States where the product has been made available
- Whether the incident is suspected of being caused by unlawful or malicious acts

Incident notification

- Within 72 hours
- The nature and an initial assessment of the incident
- Corrective or mitigating measures

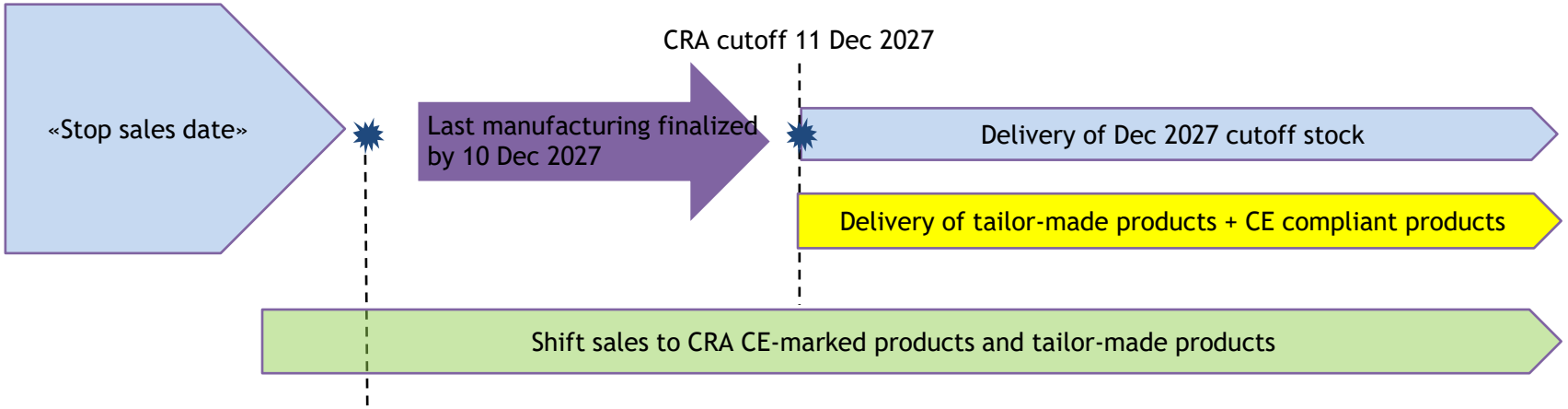
Final report

- Within one month
- Description, root cause, and mitigating measures

Authority notifications under different regulations

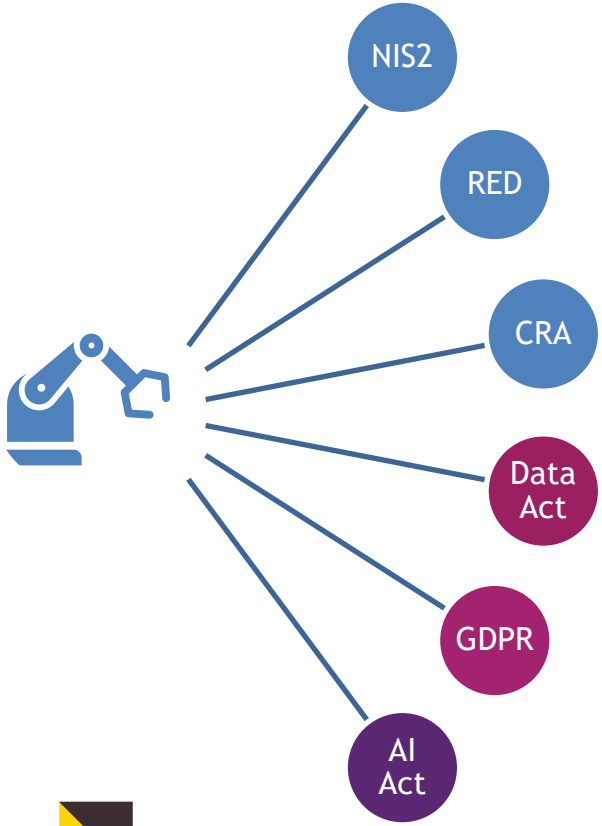
CRA	NIS2	GDPR	AI Act
CSIRT and ENISA	Market surveillance authority (in Finland) or CSIRT	Data Protection Authority	Market surveillance authority
24, 72 hours, 14 days/1 month	24, 72 hours, 1 month	72 hours	“serious incident” 15 or 10 days

Selling pre-CRA products to the EU market



Stop sales date: Last moment to start manufacturing in order to have products finished by 10 Dec 2027 (provided agreement exists)

CRA is just one piece of larger regulatory puzzle



CRA interplays with important and critical products from NIS2 environment

CRA & RED set baseline of product security

CRA contributes to data access and portability under Data Act

CRA supports compliance with Art. 32 GDPR

CRA provides presumption of AI Act compliance for PDEs qualifying as high-risk AI

New Product Regulatory Landscape

How Did Things Go? (We Really Want To Know)

Did you enjoy this session? Is there any way we could make it better? Let us know by filling out a speaker evaluation.

1. Open the IAPP Events app.
2. Select **IAPP Europe Data Protection Congress 2025**.
3. Tap "Schedule" on the bottom navigation bar.
4. Find this session. Click "Rate this Session" within the description.
5. Once you've answered all three questions, tap "Done".