PCI Security Standards Council®

2025 EUROPE COMMUNITY MEETING

2025 EUROPE COMMUNITY MEETING

Be Prepared for the Cyber Resilience Act

PCI Security Standards Council

Marcel Verstraelen

Msc Software Engineering

Senior Principal Security Evaluator

Brightsight

brightsight

An SGS company

PCI Security Standards Council

Brightsight

Our numbers

10
Locations around the globe

50+
Security standards and schemes recognitions

40
Years of experience in security evaluations

170+
Security evaluation experts

700+
Security projects performed each year

brightsight

An SGS company

European Union Cyber Resilience Act

The European Cyber Resilience Act is a mandatory EU regulation that describes the cybersecurity requirements for products with digital elements placed on the European Market

All connectable **software and hardware** products including its **remote data processing solutions** made available on the EU market that are connected either directly or indirectly to another device or to a network.

Mandatory from December 11 2027

Cybersecurity will become part of the CE marking

PCI Security Standards Council

CRA Objectives

Make sure that hardware and software placed on the EU market is **secure-by-design and secure-by-default**

Ensure **users are better informed** about cybersecurity features, support periods and known vulnerabilities

Require manufacturers to **monitor, report, and mitigate vulnerabilities and support products** with security updates throughout their lifecycle

Integrate **cybersecurity into existing CE conformity** assessment processes to simplify market access and enforcement.

CRA Key Elements

- HW and SW Product Cybersecurity requirements
- Vulnerability Handling requirements
- Technical Documentation and Instruction to user
- Conformity Assessment – differentiated by level of risk
- Supply chain security
- Reporting obligations for manufacturers

CRA Categories of Products

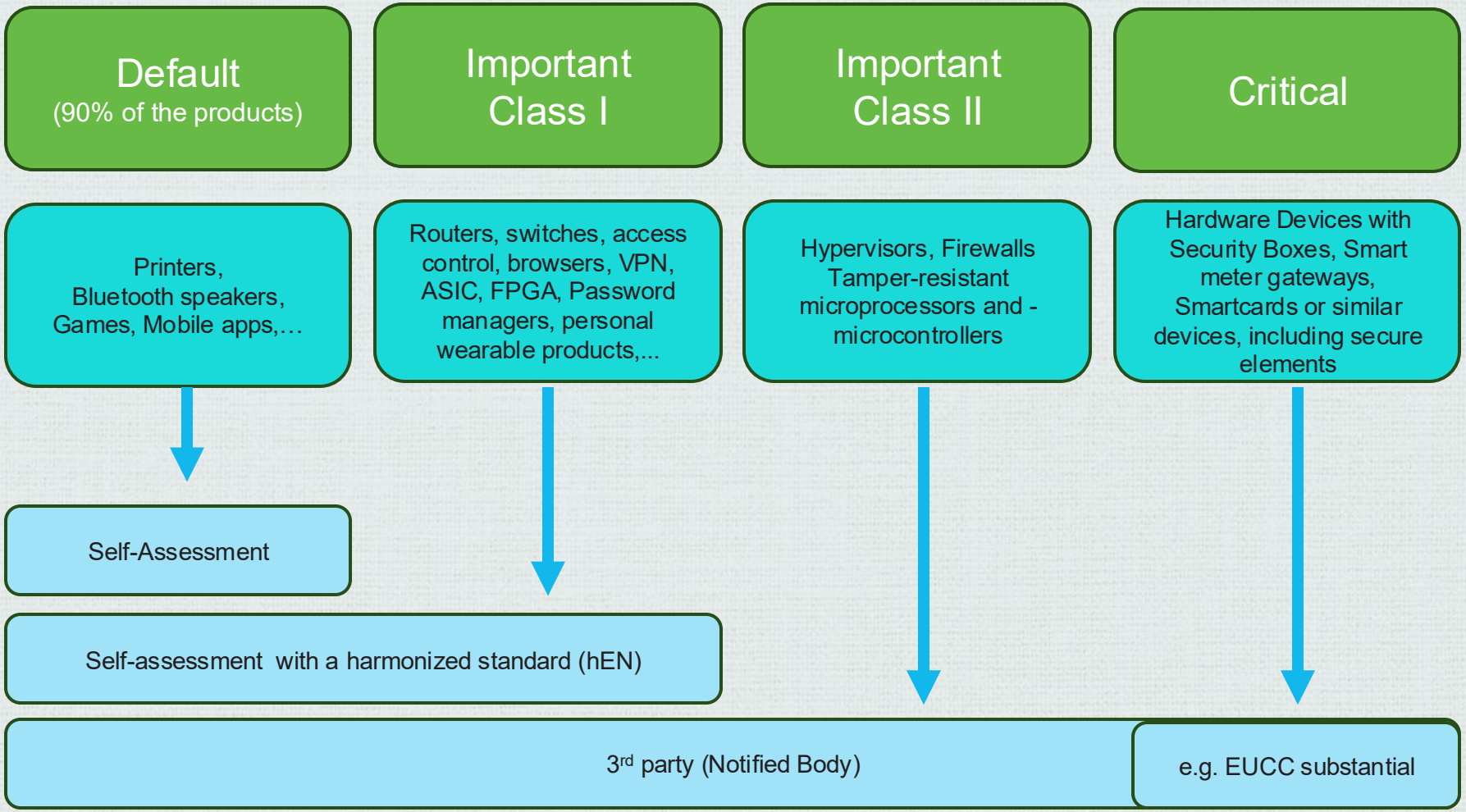
Default (90% of the products)	Important Class I	Important Class II	Critical
Printers, Bluetooth speakers, Games, Mobile apps,…	Routers, switches, access control, browsers, VPN, ASIC, FPGA, Password managers, personal wearable products,...	Hypervisors, Firewalls Tamper-resistant microprocessors and -microcontrollers	Hardware Devices with Security Boxes, Smart meter gateways, Smartcards or similar devices, including secure elements

Currently MPoC and other payment applications not (explicitly) in category Critical

NIS2 Sectors Of High Criticality: ICT system operators, organizations in the banking and financial services, energy, health, water, and transportation sectors

To be defined on December 11 2025

CRA Assessment of Products



CRA Essential Cybersecurity Requirements

Part I Cybersecurity requirements relating to the properties of products (1):

1) Products with digital elements shall be designed, developed and produced in such a way that they ensure an **appropriate level of cybersecurity based on the risks**

a) be made available **without known exploitable vulnerabilities**;
b) be made available with a **secure by default** configuration.
c) Fix vulnerabilities addressed through (automatic) **security updates**, including opt-out mechanism;
d) protection from unauthorized access
e) protect the confidentiality by **encrypting relevant data by state-of-the-art mechanisms**
f) protect the **integrity** of data

PCI Security Standards Council

CRA Essential Cybersecurity Requirements

Part I Cybersecurity requirements relating to the properties of products (2):

g. process only data to what is necessary (**data minimization**);
h. protect the availability of essential and basic functions after an incident through resilience and mitigation measures against denial-of-service attacks
i. minimize the negative impact by the products themselves on the availability of services provided by other devices or networks;
j. limit attack surfaces, including external interfaces;
k. reduce the impact of an incident using appropriate exploitation mitigation mechanisms;
l. record and monitor relevant internal activity;
m. provide the possibility to **remove on a permanent basis all data and settings**.

PCI Security Standards Council

CRA Essential Cybersecurity Requirements

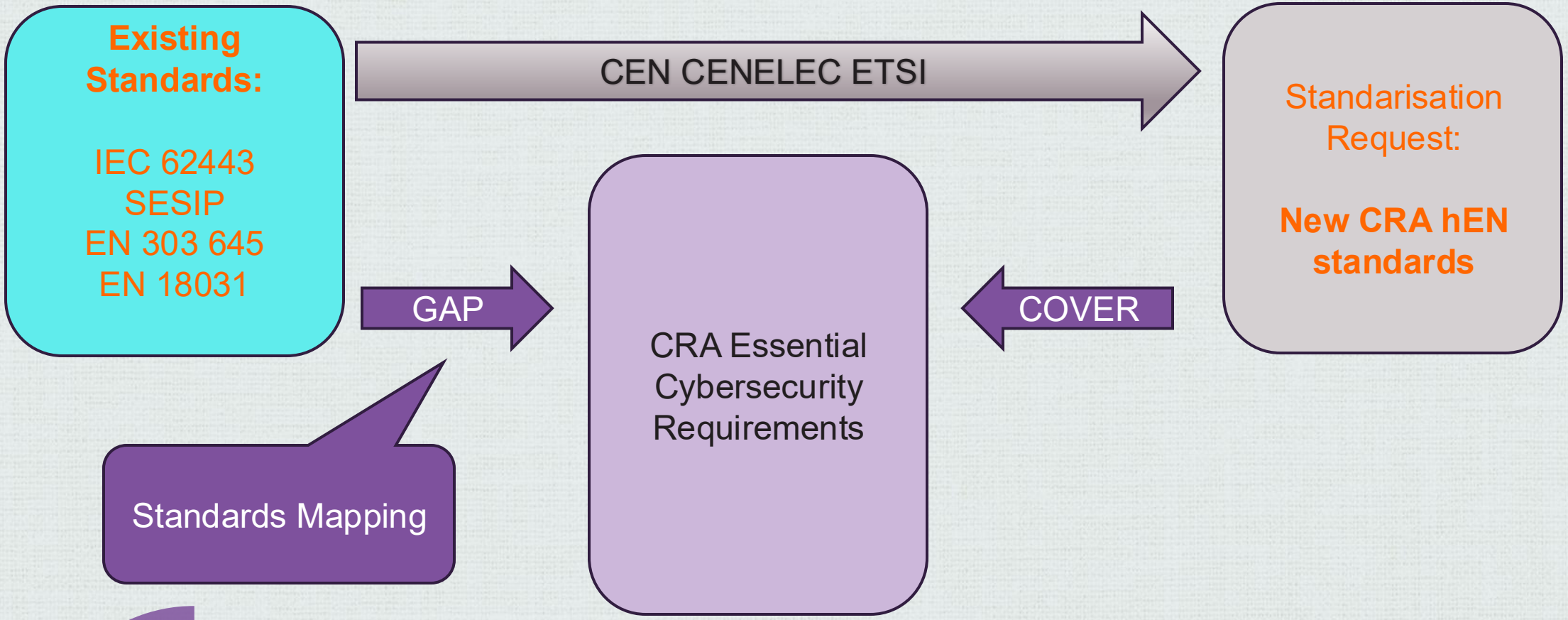
Part II Vulnerability handling:

Ensure that there is a process in place to maintain the device security during its life cycle

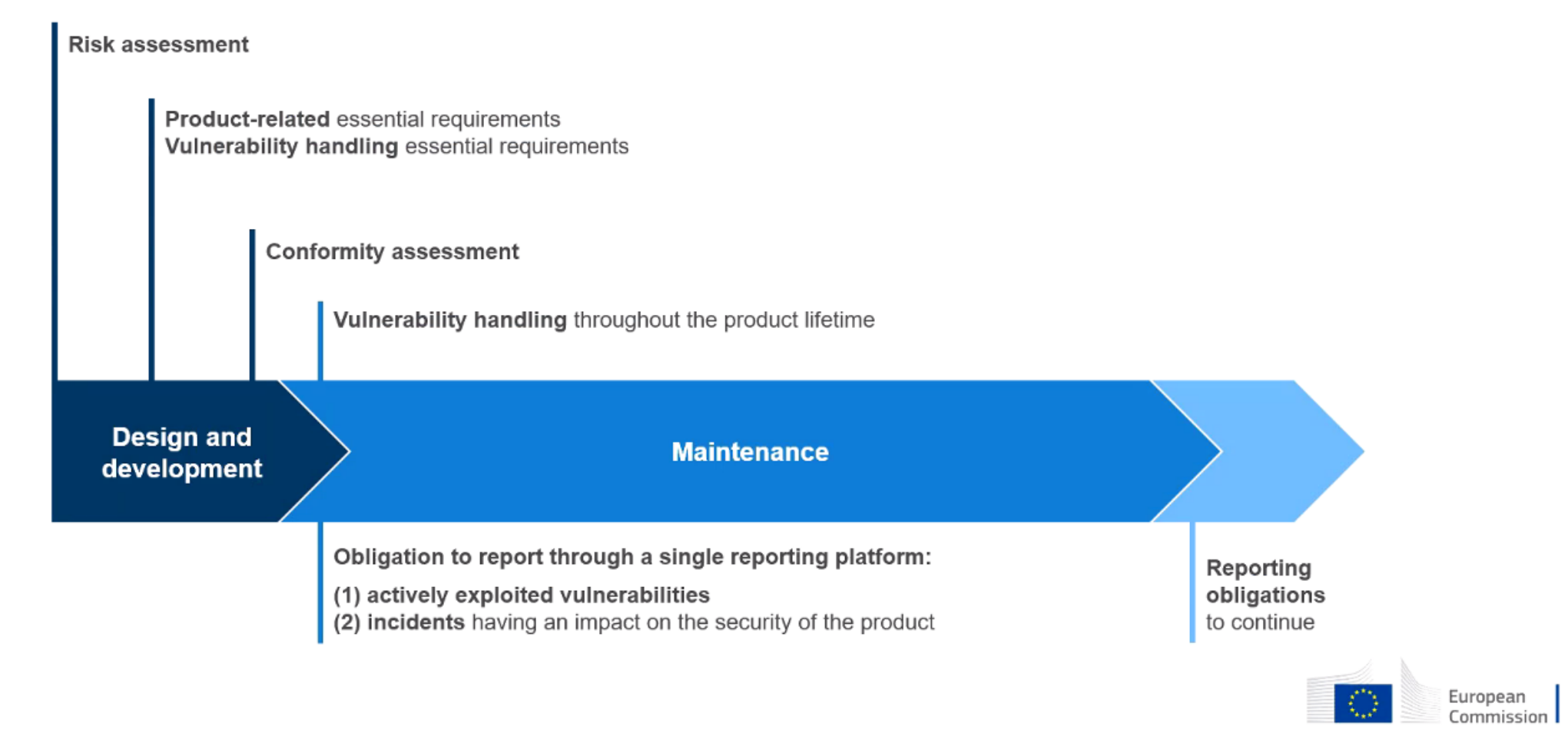
1. **document vulnerabilities and components** including a software bill of materials (SBOM);
2. provide **security updates**;
3. apply **regular tests**
4. publicly **disclose information about fixed vulnerabilities**
5. put in place and enforce a **policy on vulnerability disclosure**;
6. **facilitate the sharing of information about potential vulnerabilities** in the product as well as in third-party components
7. securely **distribute updates**.
8. security updates are disseminated **without delay**.

Mapping to CRA Requirements

Standards under development that define how to assess a device



CRA and Your Development Process



CRA and PCI Standards

PCI PTS / MPoC / S3:

- Requirements on Vulnerability management process
- Requirements on development process
- Requirements on device/software security implementation

Many requirements of CRA overlap with PCI requirements;

- i.e. When doing a PCI evaluation, several CRA requirements are already covered
  - Less time, less cost during

Gap between PCI and CRA then needs to be assessed

Brightsight CRA Services

How we can support you in achieving CRA listing:

- Explain scope and product categories for CRA
- Conformity Assessment Procedures that are available for the product(s)
- Gap analysis between CRA requirements and standards that are used for current certifications
- Review Cybersecurity Risk Assessment
- Process and Documentation requirements for CE marking
- Obligations during support period (maintenance, vulnerability handling and reporting)

CRA and Radio Equipment Directive

Currenty applicable Radio Equipment Directive

Also EU regulation

From August 2025

Overlap between RED requirements and PCI (PTS)

CRA will replace RED from 11 december 2027

Take Aways

CRA is mandatory from December 11 2027

Though not all is set in stone yet

Make sure you know what to do to reach CRA compliance?

PCI approved products, have already parts of the CRA requirements covered

Brightsight can support you in the process:

- developer & advisory support
- Re-use of PCI evaluations (PCI PTS, PCI MPoC….)
- Evaluation and certification of your product

PCI Security Standards Council