The Cyber Resilience Act (CRA)

What You Need to Know & How to Prepare

Navigating the Regulatory Landscape for Product Cybersecurity

—

18 September 2026

Presenters

Edouard de Schietere de Lophem

KPMG Advisory

Advisor

Cyber Security Services

T +32 27 08 43 00
M +32 474 28 69 90
E edeschieteredelophem@kpmg.com

Raf Schoefs

KPMG Law

Senior Counsel

Technology, IP & Data

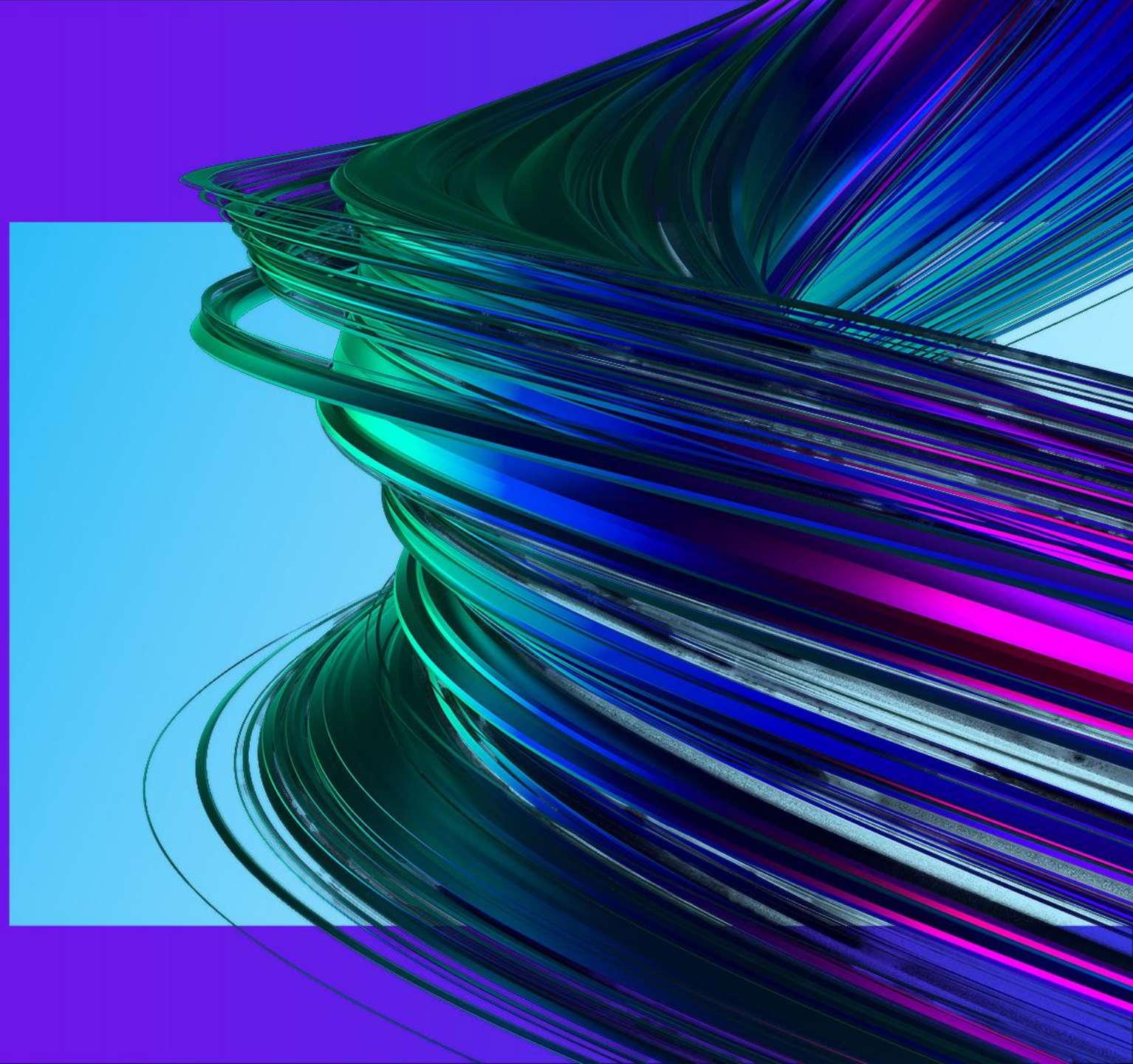
T +32 27 08 44 00
M +32 475 42 93 36
E : rschoefs@kpmglaw.be

Agenda

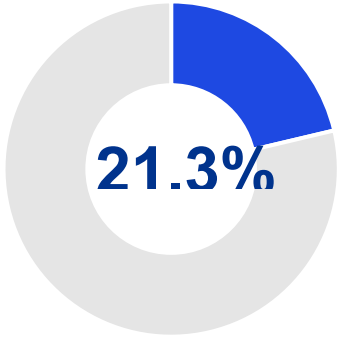
1. Introduction
2. Scope of the CRA
3. CRA obligations and enforcement
4. Timelines and implementation
5. Key Takeaways

1.

Introduction

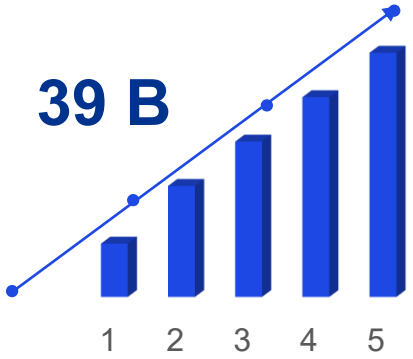


Why the CRA matters



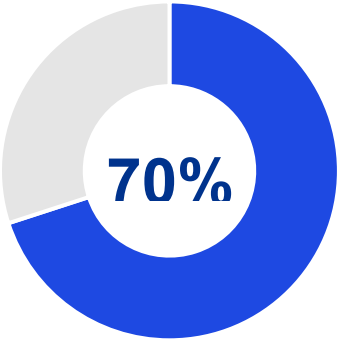
Of observed incidents involved vulnerability exploitation

ENISA threat Landscape 2025



Connected IoT devices expected by 2030

IoT Analytics forecast

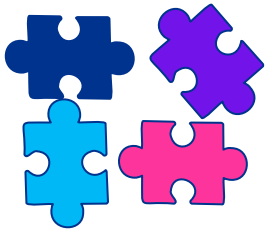


Of vulnerability cases culminate in intrusions

ENISA threat Landscape 2025

No prior EU-wide regulation

No EU-wide regulation specifically addressed the cybersecurity of products with digital elements (PDEs).



Existing rules were fragmented

Requirements were spread across different frameworks or limited to specific sectors and product types

Limitations of NIS and RED

They did not fully address lifecycle product cybersecurity for all products with digital elements.

What is the CRA?

EU-wide regulation
One framework across the EU internal market.
Regulation (EU) 2024/2847

Products with digital elements (PDEs)
Covers connected hardware and software.

Product lifecycle approach
Cybersecurity requirements from design to end-of-life.

OBJECTIVES

Secure products throughout the lifecycle

Improves cybersecurity from product design through end-of-life.

Harmonise EU rules

Sets common cybersecurity requirements across the EU internal market.

Clear accountability across the value chain

Sets manufacturer, importer and distributor responsibilities across the lifecycle.

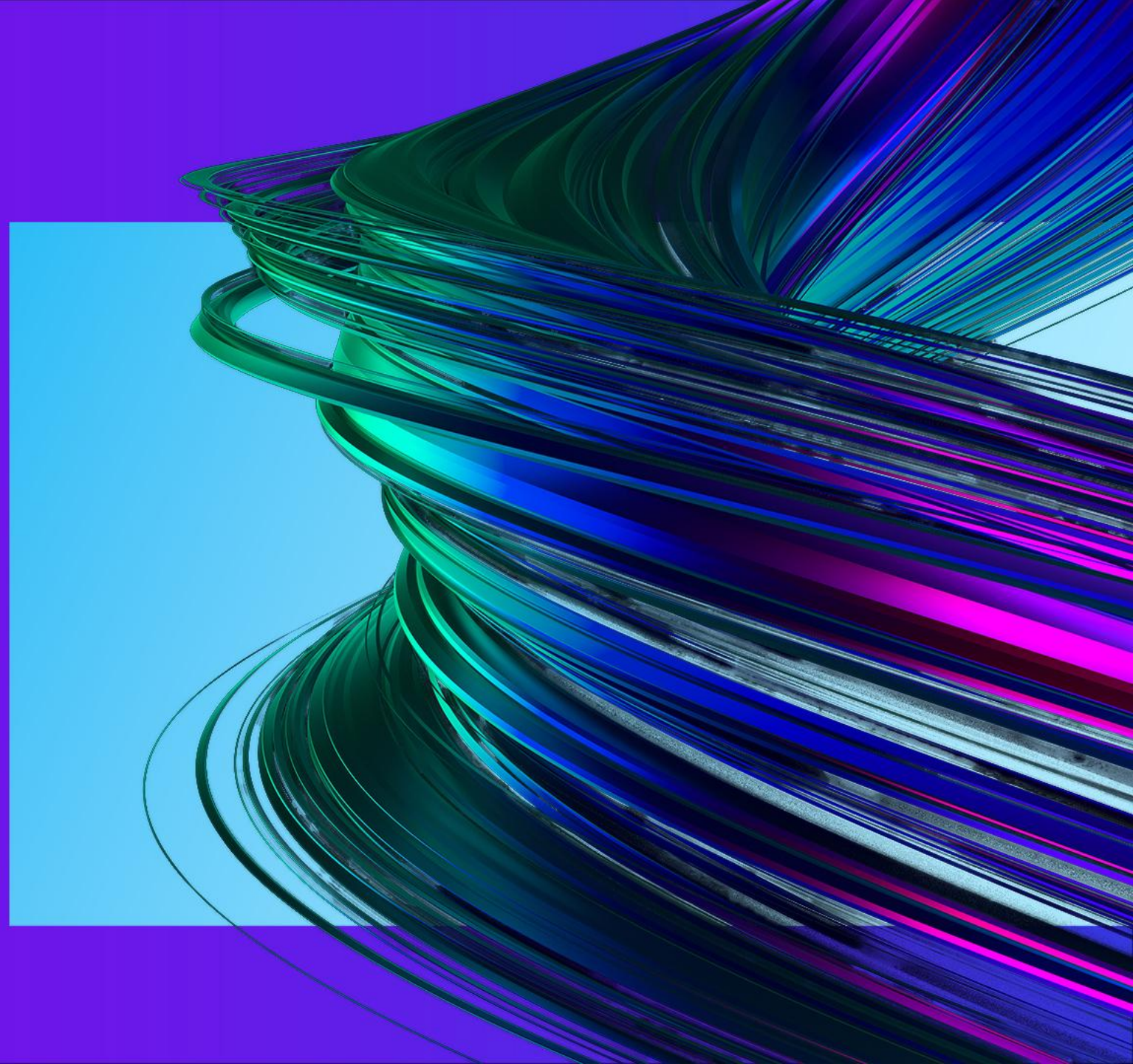
Transparency for users and buyers

Clarifies security information, documentation, support and update commitments.

KPMG

2.

Scope of the CRA



Scope of the CRA

1. Products in Scope

- Products with digital elements that are directly or indirectly connected to another device or network and made available on the market in the course of a commercial activity

This also includes both hardware and software

2. Examples

- Smartphones, routers, webcams
- Operating systems

It also includes cloud-based applications (when they meet the remote data processing test), smart devices such as TVs, AI-enabled devices.

4. Territorial Scope

- Applies to in-scope products placed on the EU market, regardless of origin

This includes products and services manufactured outside EU (e.g. China, US, etc.).

3. Products Excluded

- Certain products are excluded or assessed separately

See subsequent slides for key exemptions and carve-outs

Examples of products likely in scope (1/2)

Connected hardware

- Routers and modems
- Smart cameras and smart meters
- Connected toys and smart home devices
- Industrial / manufacturing IoT devices

Security / network production

- Firewalls
- Password managers
- Network controllers
- Endpoint security software

Standalone Software

- Desktop applications
- Mobile applications
- Operating systems
- Accounting or business software

Related remote data processing solutions

- Cloud or remote processing linked to a product
- Remote monitoring or management solutions tied to a product with digital elements
- Companion back-end services supporting a connected product

Examples of products likely in scope (2/2)

Mobile banking application

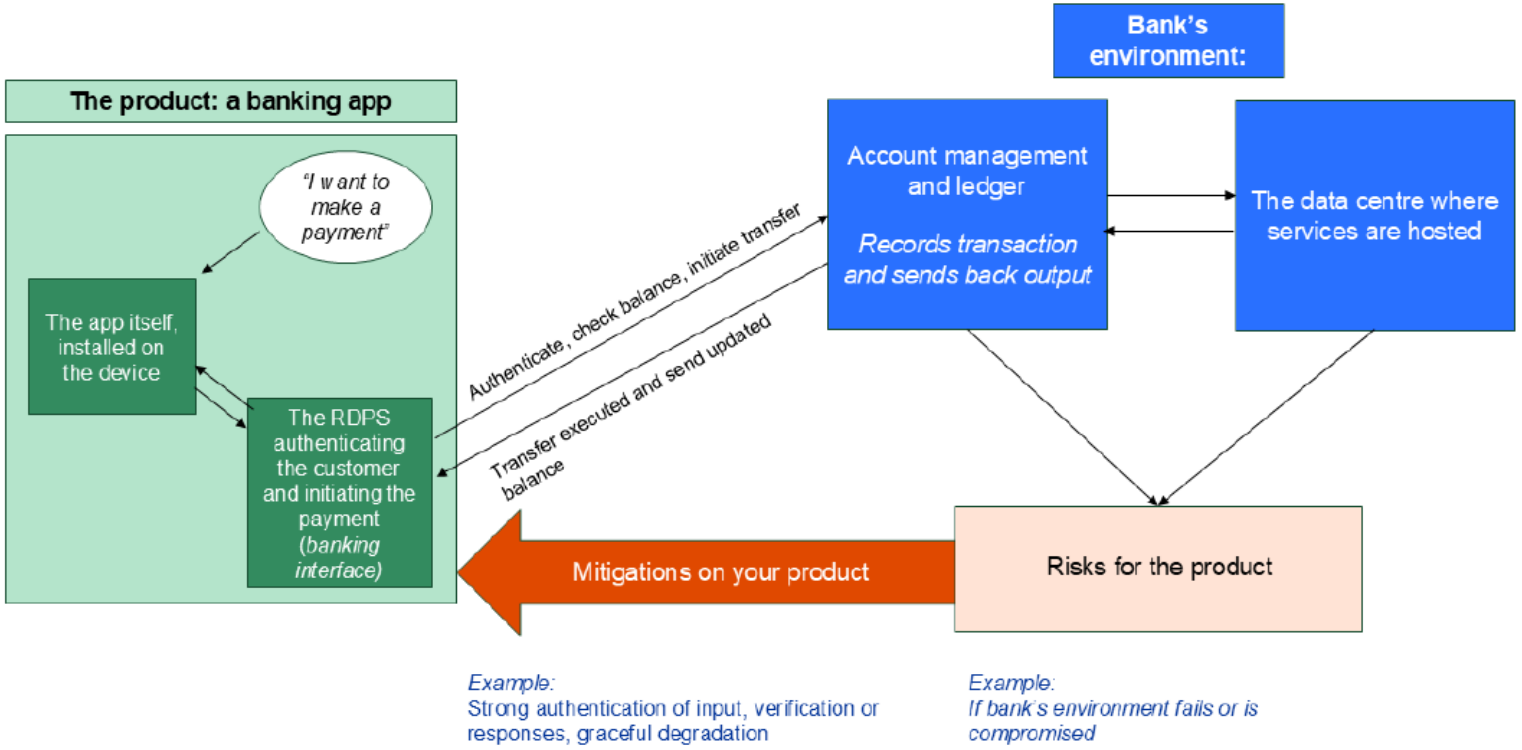


Figure 10: Stylised representation of a banking app relying on RDPS

Main exemptions and special cases

Non-commercial open-source software

- Developed outside a commercial activity
- No monetization or paid support
- Assess carefully if commercial elements are involved

Pure Services / certain SaaS

- The CRA is a product law
- Assess separately if linked to a product with digital elements

Products covered by other EU rules

Medical devices (Regulation 2017/745)

Motor vehicles (Regulation 2019/2144)

Civil aviation (Regulation 2018/1139)

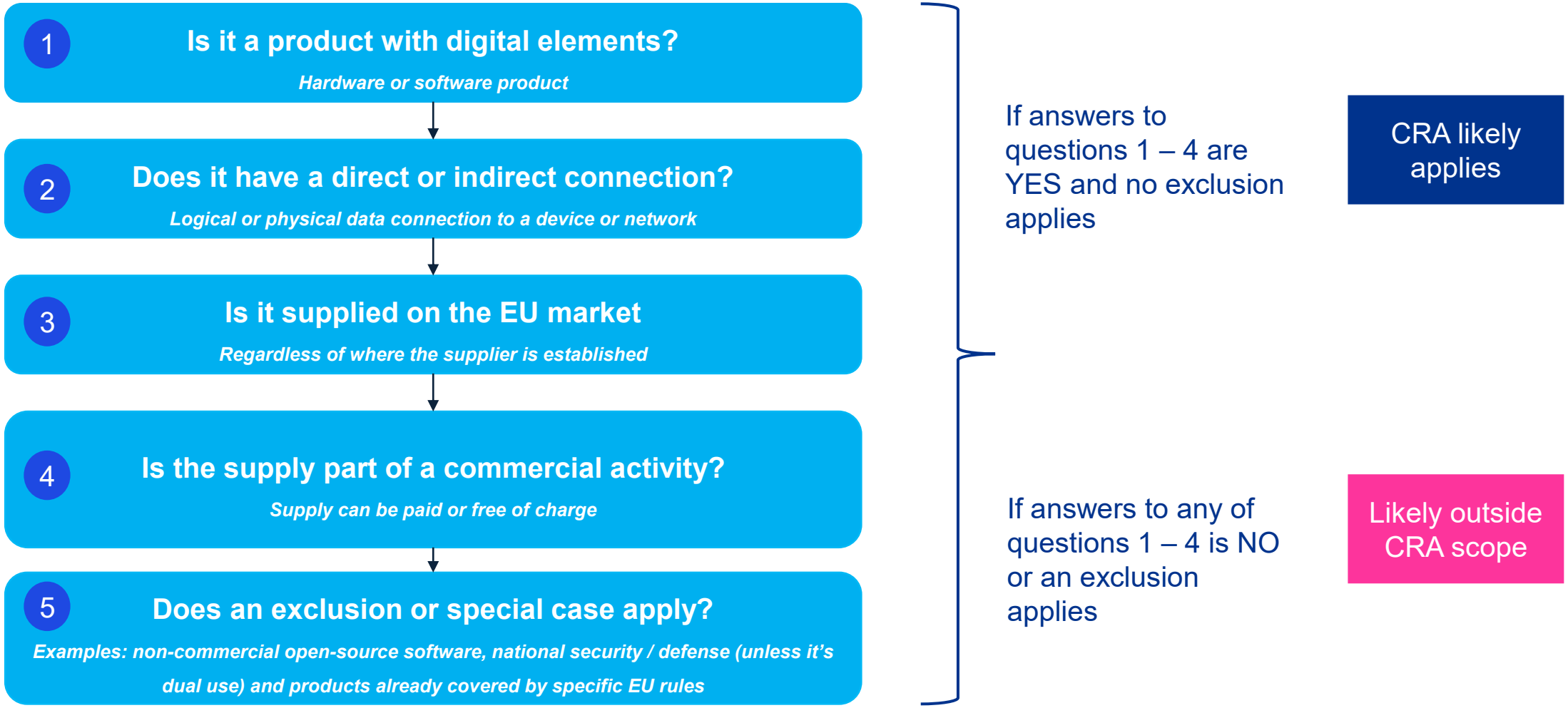
Marine equipment (Directive 2014/90)

Medical diagnostic (Regulation 2017/746)

Other exclusions / special cases

- Products exclusively developed for national security or defense purpose
- Certain prototypes and unfinished testing software

CRA scope assessment



Cyber Resilience Act Ecosystem

European Commission
- Sets the CRA rules, adopts delegated acts, oversees market surveillance, and ensures consistent enforcement across the EU.

ENISA
- Supports the Commission and Member States with technical expertise, cybersecurity guidance, and coordination on vulnerability handling.

Market Surveillance Authorities
- Designated by EU Member States to enforce CRA compliance.
- Conduct inspections, monitor incidents, and apply penalties for non-compliance

Notified Bodies (CABs)
- Independent third-party organizations authorized to assess high-risk products.
- Evaluate and certify that critical PDEs meet CRA security standards.

Key Players with Obligations under CRA

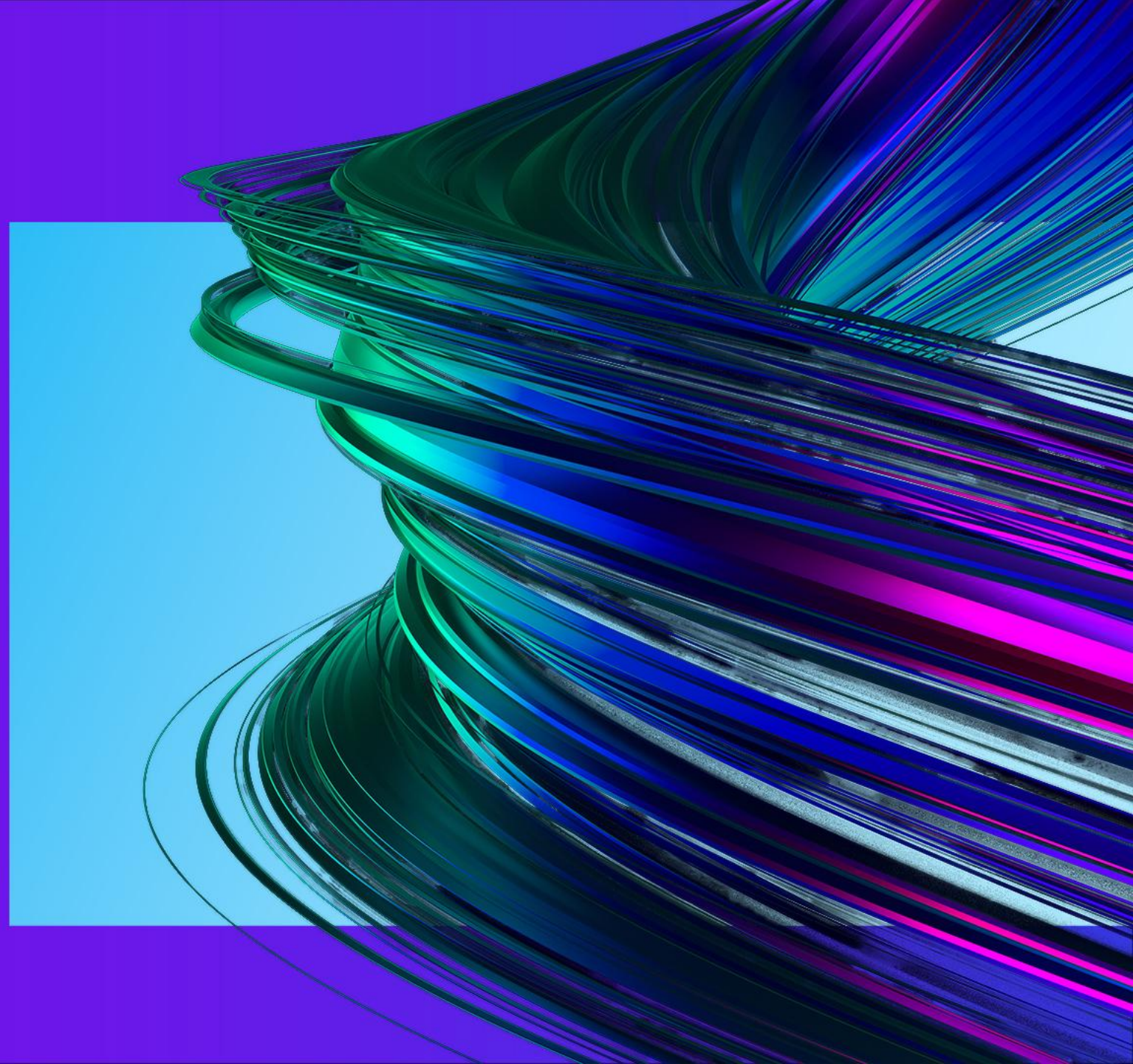
- Manufacturers
- Importers
- Distributors
- Open-source software stewards

Consumers and Business End-Users
- Indirectly impacted by increased security and transparency.
- Will benefit from products with better cybersecurity, longer update support, and improved risk communication.
- Will translate CRA requirements in procurement processes and contractual requirements

KPMG

3.

CRA obligations and enforcement



Key obligations of the different economic operators

01

Manufacturers' key obligations

- Vulnerabilities prevention & management
- Data protection & management
- Risk assessment
- Security configuration
- Resilience and Protection against cyberattacks
- Monitoring of the product with digital elements

02

Distributors' key obligations

- Due Care in Compliance
- Pre-Market Verification
- Conformity Assessment
- Corrective Actions for Non-Compliance
- Cooperation with Authorities
- Notification on Manufacturer Cessation

03

Importers' key obligations

- Market Compliance
- Conformity Verification
- Risk Management and Notification
- Contact Information
- Corrective Actions and Communication
- Documentation and Cooperation

04

Open-source software stewards' key obligations

- Establish and Document a Cybersecurity Policy
- Promote Vulnerability Reporting and Handling
- Cooperate with Market Surveillance Authorities
- Provide Documentation to Authorities upon Request
- Address Security Incidents
- Comply with Development Obligations

CRA Products' Classification

Category	1. Default category	2. Important Products Class I	3. Important Products Class II	4. Critical Products
	Covered by CRA, but not listed in Annex III or Annex IV	**Cybersecurity-relevant products listed in Annex III**	**Higher-impact cybersecurity products listed in Annex III**	**Highest category, linked to possible EU cybersecurity certification**
Examples	• Memory chips • Mobile apps • Smart speakers • Computer games • ….	• Password Managers • Operating Systems • Routers, modems and switches • Smart home security • SIEM systems • …	• Hypervisors and container runtime systems • Firewalls • Intrusion detection and prevention systems • Tamper-resistant microprocessors • …	• Hardware devices with security boxes • Smart meter gateways • Smartcards or similar devices, including secure elements • …

The product category determines which conformity assessment path applies.

CRA Standards

Note
- Horizontal standards (everyone)
- Vertical standards (only important/critical products)
- Common specifications (if no harmonized standard exists)

Common Specification

Recognized frameworks for "default" products

- IEC 62443 Operational Technology
- EN 303 645 Consumer IoT

Vertical Standards

Specific for "important" and "critical" product

- Password Manager
- Anti-virus
- Network interface
- Firewall
- Secure element

Horizontal Standards

process related and generic

- Secure development lifecycle (SDLC)
- Vulnerability handling & disclosure processes
- Secure-by-design and secure-by-default principles
- Documentation, logging, and patching practices

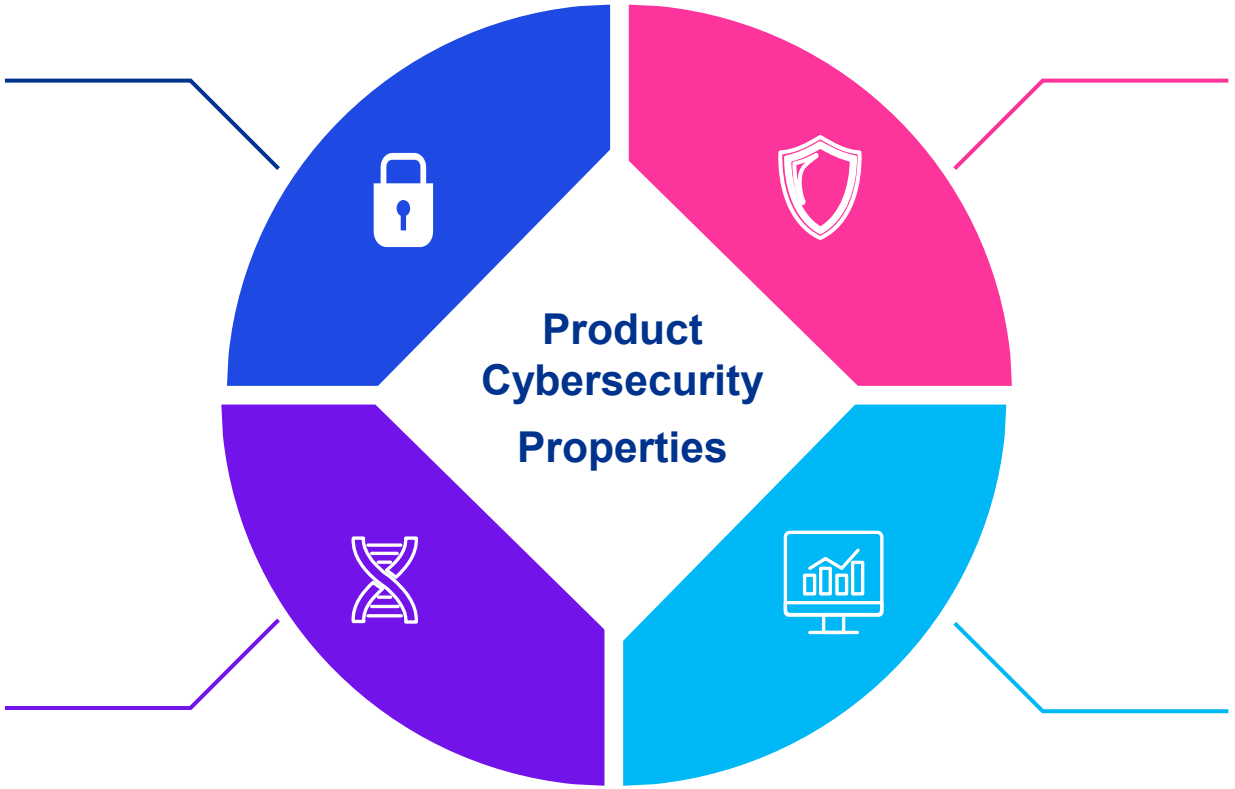
Essential Cybersecurity Requirements – Annex I, Part I

Secure by design and by default

- Risk-based level of cybersecurity
- No known exploitable vulnerabilities at market placement
- Secure default configuration

Remain resilient in operation

- Availability of essential functions
- Reduced impact on connected devices or networks
- Limited attack surface and external interfaces



Protect access and data

- Protection against unauthorized access
- Confidentiality & integrity of data
- Data processing limited to what is necessary

Support traceability and user control

- Security-relevant activity can be recorded or monitored
- Users can securely remove data and settings

Vulnerability Handling Requirements– Annex I, Part II

01

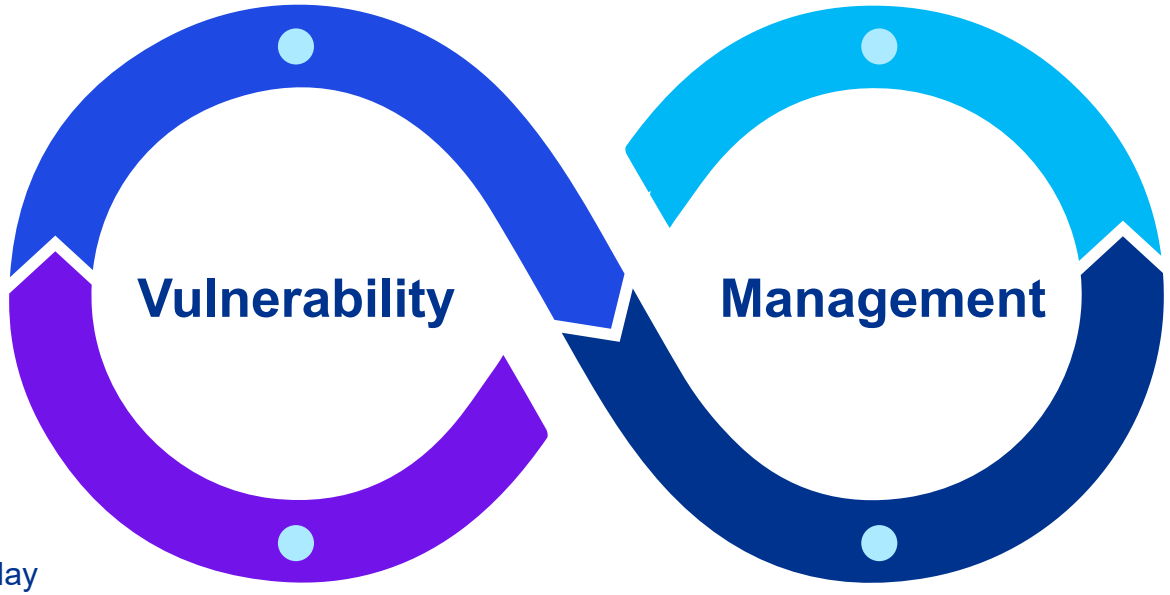
Identify and document

- Identify vulnerabilities and product components
- Maintain a Software Bill of Materials (SBOM)
- Track relevant dependencies

02

Review and Test

- Regularly review product security
- Test the product for vulnerabilities
- Monitor security issues during the support period



03

Remediate and update

- Address vulnerabilities without undue delay
- Provide security updates where needed
- Make security updates available free of charge

04

Disclose and coordinate

- Maintain a Coordinated Vulnerability Disclosure policy
- Facilitate vulnerability reporting
- Share information on fixed vulnerabilities

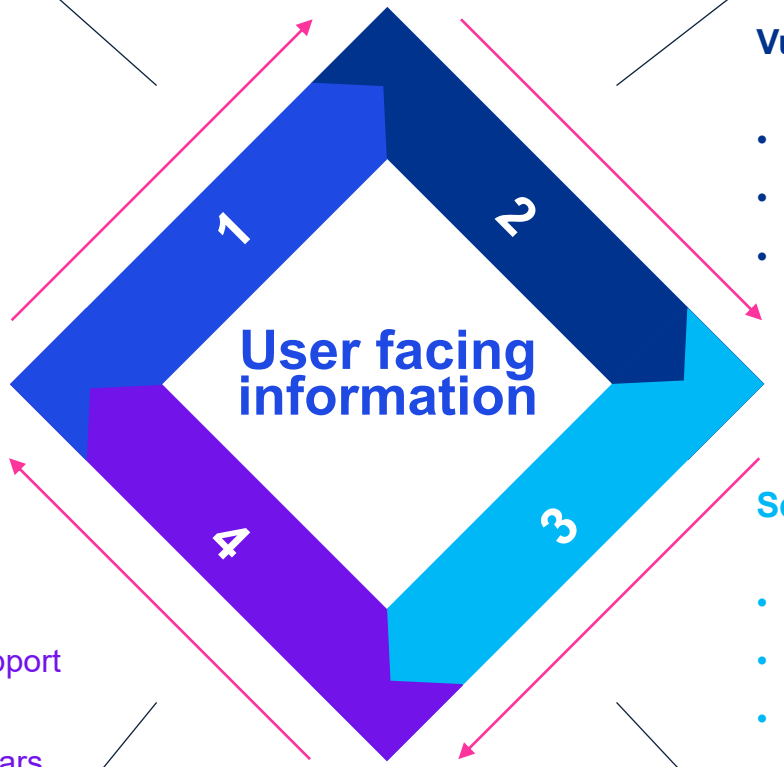
Essential Cybersecurity Requirements – Annex II

Product & manufacturer identification

- Product name, type and version
- Manufacturer name and contact details
- Intended purpose and use environment

Support period & updates

- End date of the support period
- Security updates provided during support period
- Support period normally at least 5 years
- Updates made available free of charge



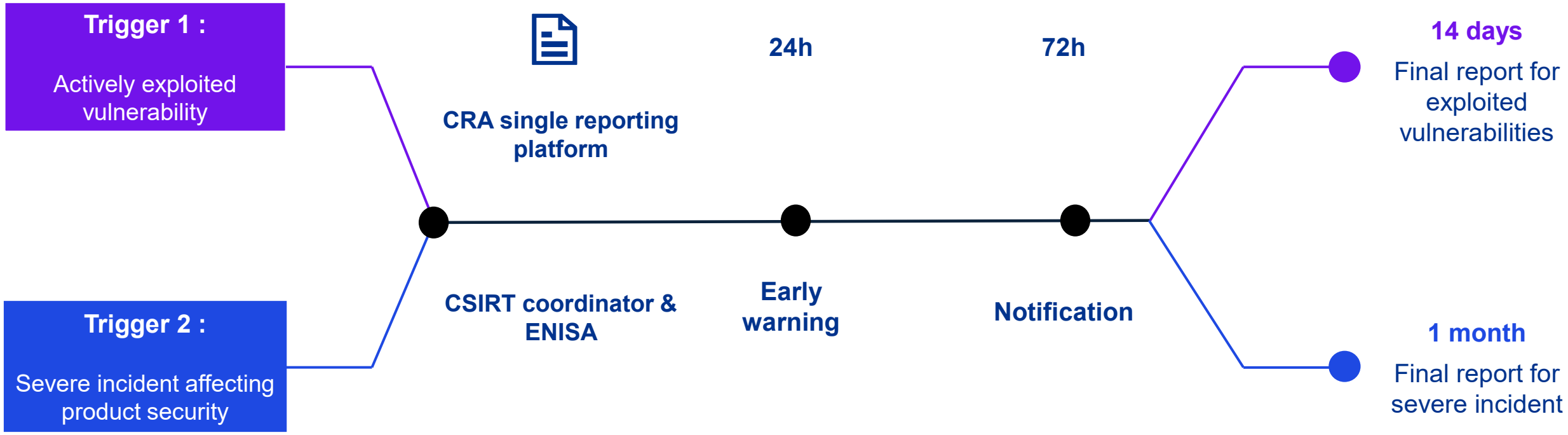
Vulnerability contact & reporting

- Single point of contact
- How vulnerability can be reported
- Where the CVS policy can be found

Secure use & availability

- Secure installation and configuration
- Secure decommissioning and data removal
- User information kept available for 10 years after market placement, or the support period If longer

When does reporting apply ? – Article 14



EU Declaration of Conformity – Annex V

What is it?

- Formal legal statement by the manufacturer
- Confirms that the product complies with the Cyber Resilience Act
- Issued under the manufacturer's sole responsibility
- Required before CE marking & EU market placement

A simplified version also exists

01 Product identification

Name, type, version or other info enabling unique identification

02 Manufacturer details

Name and address (or authorised representative)

03 Responsibility statement

Declaration issued under sole responsibility of the manufacturer

04 Object of the declaration

Clear identification of the product (traceability; may include photo)

05 Compliance statement

Confirmation that the product complies with relevant EU legislation (incl. CRA)

06 Standards / specifications applied

References to: Harmonised standards, Common specifications and/or Cybersecurity certification (if used)

07 Conformity assessment details (if app)

Notified body name & number, assessment procedure performed and certificate identification

08 Signature & formalities

Place & date of issue, name & function of signatory and signature

Technical Documentation (Annex VII)

Purpose

- Demonstrates compliance with CRA essential requirements
- Enables conformity assessment and MSA verification

Product description

- Intended purpose, architecture, components (HW/SW)

Design & development

- Secure development lifecycle (SDLC)
- Security-by-design / default implementation

Risk assessment

- Threats, vulnerabilities, mitigation measures

Cybersecurity controls

- Mapping to Annex I requirements

Testing & validation

- Security testing, verification results

SBOM

- Components, dependencies, versioning

Vulnerability handling

- Processes, tools, timelines

Update & support policy

- Support period, patching approach

Key principles

1. Living document (updated during lifecycle)
2. Traceable & auditable
3. Available without undue delay to MSAs

Procedure (Conformity Assessment – Annex VIII / Article 32)

Step 1 — Product classification

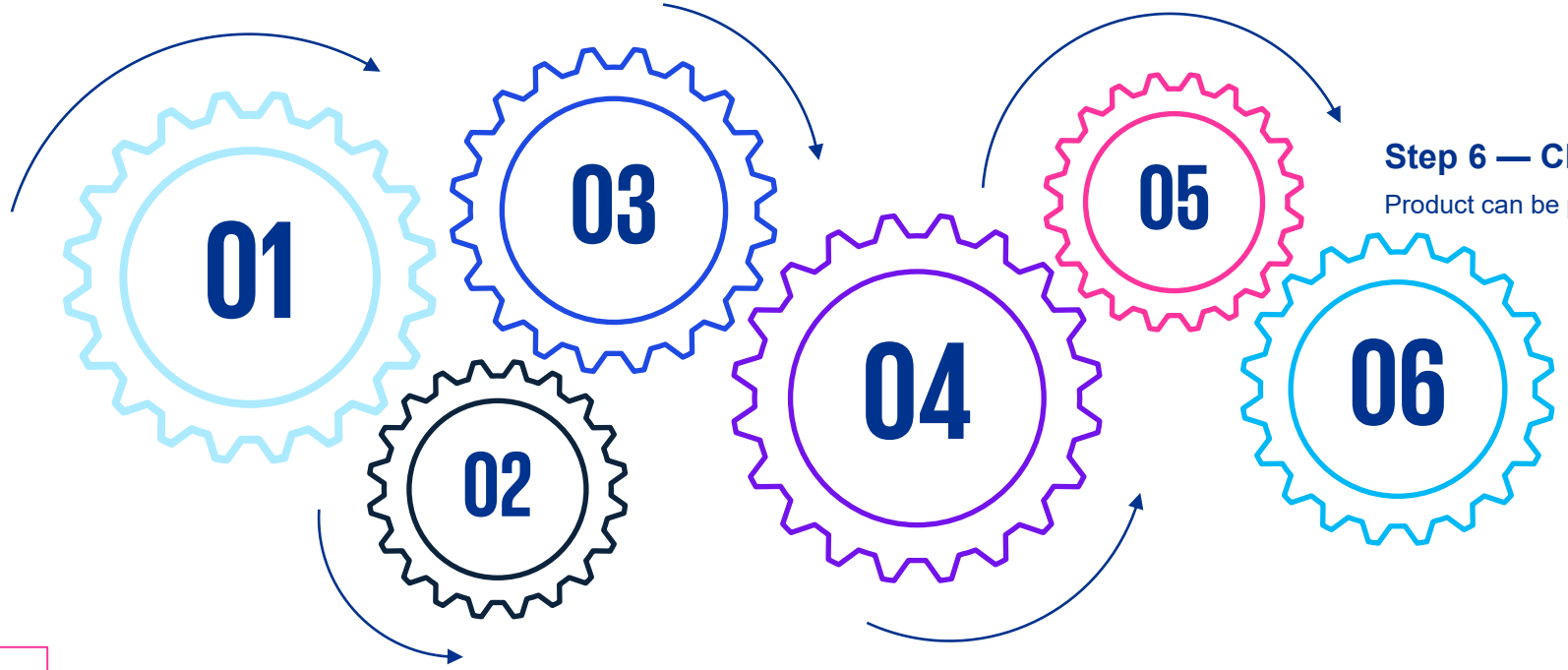
- Default /
- Important (Class I / II) /
- Critical

Step 3 — Demonstrate compliance

- Apply harmonised standards / common specs
- Perform testing & verification

Step 5 — EU Declaration of Conformity

- Formal manufacturer statement



Step 6 — CE marking & market placement

Product can be placed on EU market

Higher risk products may require mandatory third-party involvement (Notified Body)

Step 2 — Select conformity route (Art. 32)

- Module A: Self-assessment (internal control)
- Module B + C: Type exam + production control
- Module H: Full quality assurance system

EU Cybersecurity Certification (if applicable)

Step 4 — Compile technical documentation

- Annex VII complete file

CRA enforcement and penalties

01 Who enforces?

- National Market Surveillance Authorities (MSAs)

02 Trigger events?

- Reported vulnerabilities / incidents
- Complaints (users, competitors)
- Targeted MSA campaigns
- ENISA / CSIRT information sharing

03 MSA powers

- Request technical documentation
- Conduct compliance checks / product testing
- Request corrective actions
- Order withdrawal / recall / market ban

Administrative fines (key figures)

Key infringements / requirements	Up to €15M OR 2.5% global annual turnover
Other specified CRA obligations (Arts. 18-23, 28, 30-33, etc.)	Up to €10M OR 2% global annual turnover
Incorrect / misleading information	Up to €5M OR 1% global annual turnover

Additional enforcement measures

- Product withdrawal or recall from the EU market
- Sales restrictions or market bans
- Mandatory corrective actions (e.g. patching, remediation)

How penalties are determined

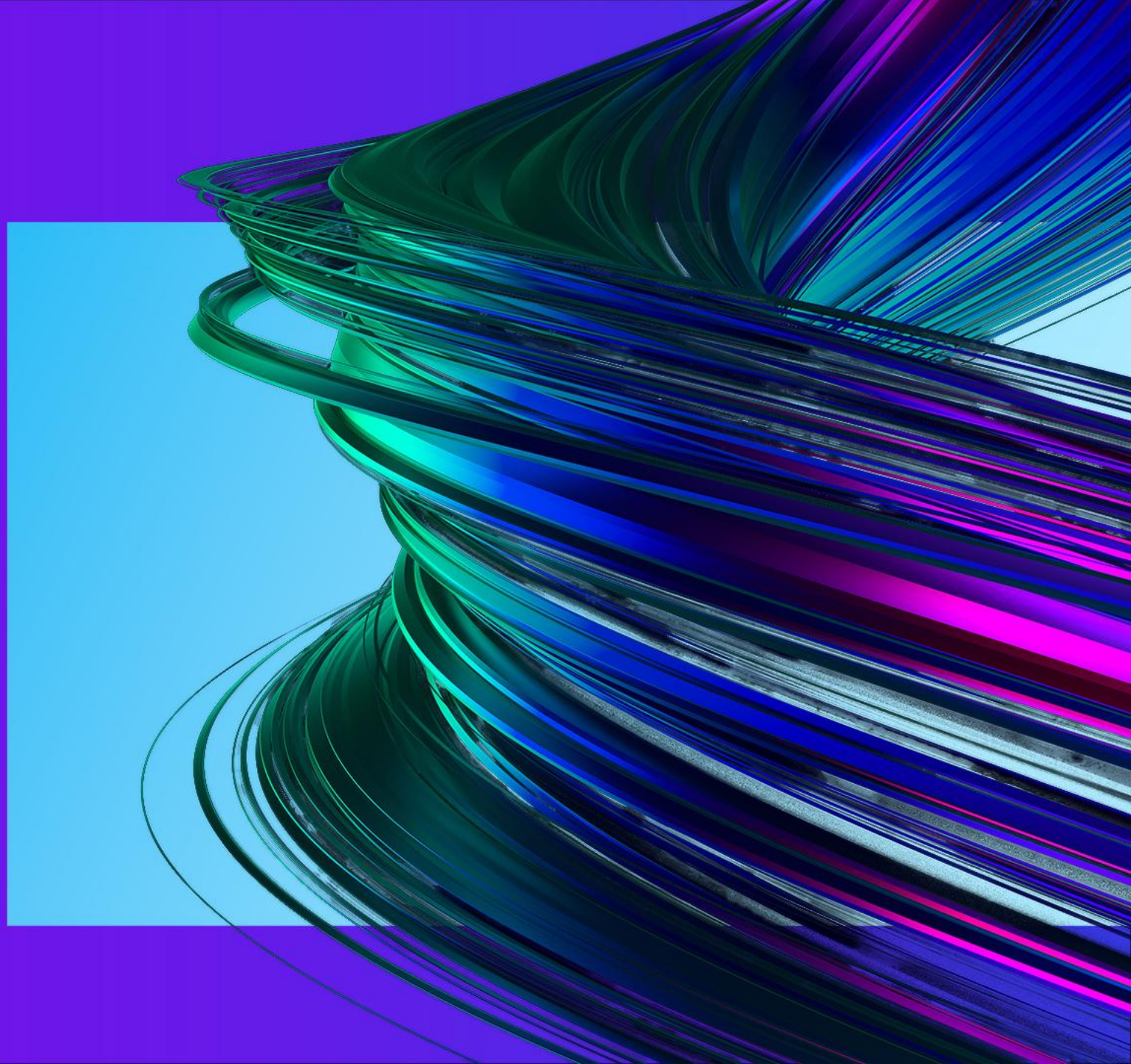
- Nature, gravity, duration and consequences of the infringement
- Previous administrative fines for a similar infringement
- Size and market share of the company

Post-market phase is actively monitored — not a one-time compliance.

KPMG

4.

Timelines and implementation



CRA timelines

11 Jun 2026

Conformity assessment framework applies

(Chapter IV – Notification of Conformity Assessment Bodies)
Member States designate notifying authorities and rules on the notification of conformity assessment bodies become applicable.

11 Sep 2026

Vulnerability & incident reporting obligations apply

Mandatory reporting obligations under Article 14 become applicable for manufacturers.

30 Oct 2026

Product-specific standards (expected)

Standards for categories such as OT, smart home, browsers, VPNs, password managers, etc. expected to be available.

30 Oct 2027

Further horizontal standards expected

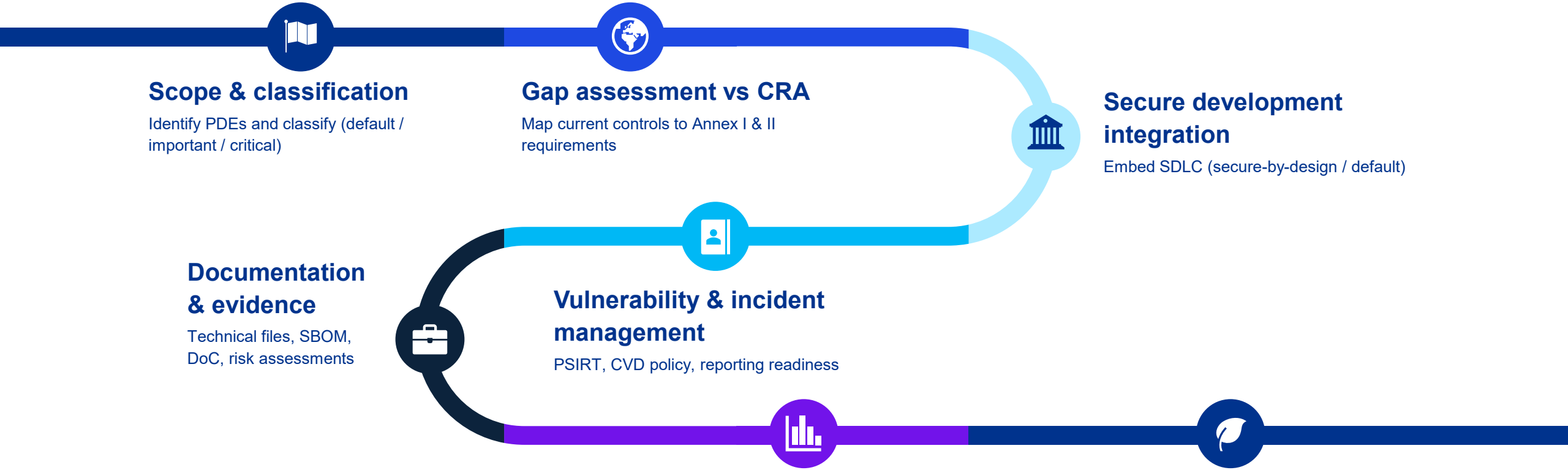
Final harmonised standards package (supporting the Annex I requirements) expected to be completed.

11 Dec 2027

Full CRA applicability

Core CRA requirements become fully applicable, including essential cybersecurity requirements (Annex I), conformity assessment and CE marking.

Steps to CRA Readiness



Scope & classification

Identify PDEs and classify (default / important / critical)

Gap assessment vs CRA

Map current controls to Annex I & II requirements

Secure development integration

Embed SDLC (secure-by-design / default)

Vulnerability & incident management

PSIRT, CVD policy, reporting readiness

Documentation & evidence

Technical files, SBOM, DoC, risk assessments

Governance & operating model

Roles, accountability, training

Market surveillance readiness

- Centralised documentation
- Rapid response capability (MSA requests)

Existing frameworks and CRA gaps

Prepare for market surveillance

- Centralised technical documentation
- Living SBOM & risk files
- Internal playbooks for MSA requests

Leverage existing frameworks

CRA is not a new system but a structured reuse of existing frameworks

CRA Requirement	Existing Framework to Leverage
Governance & risk	ISO 27001 / NIST CSF 2.0
Secure development	IEC 62443-4-1 / NIST SSDF
Vulnerability management	ISO 30111 / ISO 29147
Product testing	IEC 62443, ETSI standards
Supply chain	SBOM (Cyclone DX / SPDX)
Incident reporting	NIS2 processes + PSIRT

CRA documentation expectations

01

Core Documentation set

- Technical documentation (Annex VII)
- Risk assessment
- SBOM
- Vulnerability handling procedures
- Update & support policy
- EU DoC

02

Retention & availability

- Retention: ≥ 10 years after market placement
- Availability: without undue delay to MSAs
- Dynamic: continuously updated during support period

03

Common pitfalls

Documentation exists but:

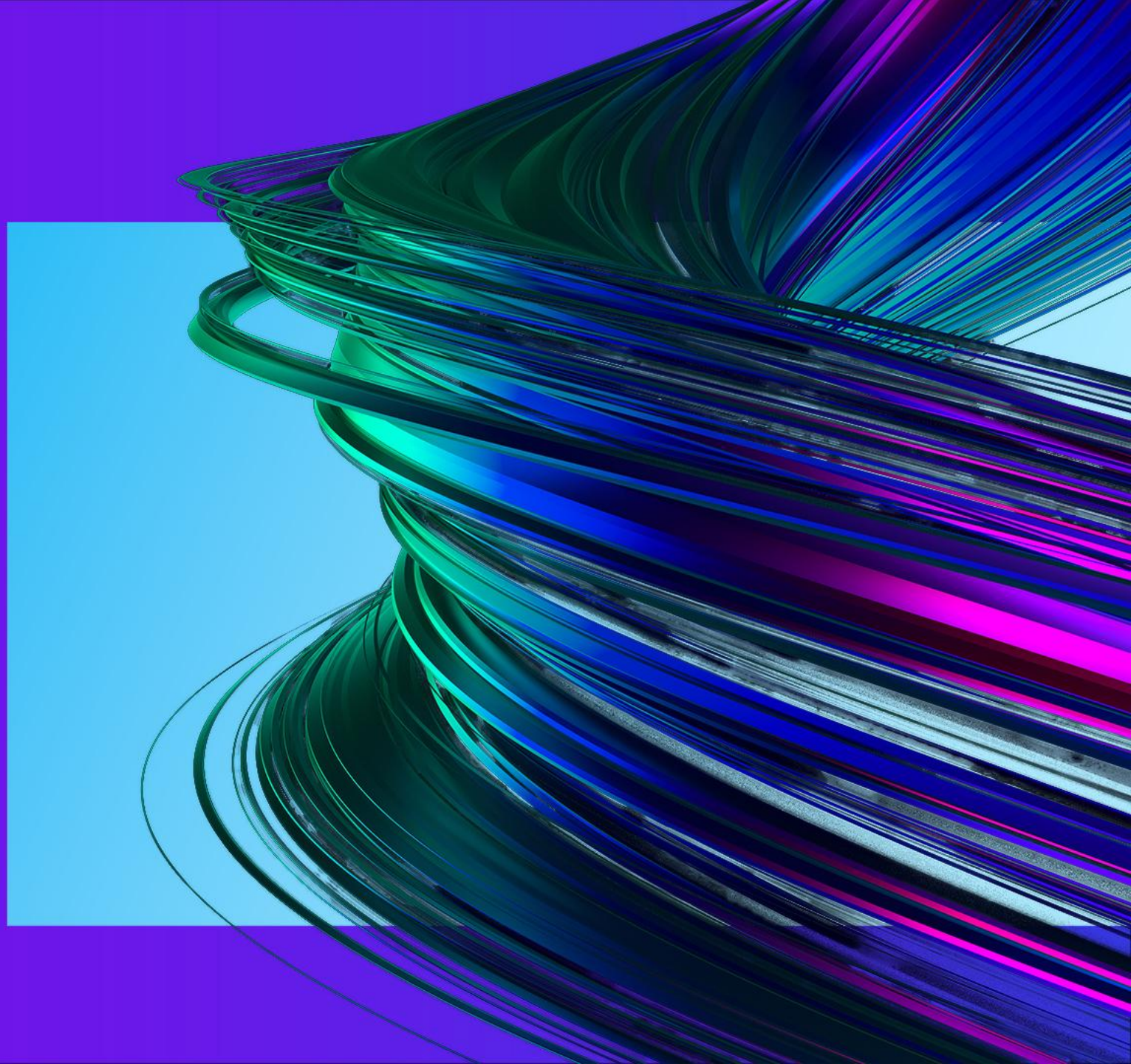
- Not centralized
- Not updated
- Not audit-ready

Documentation is to be maintained up to date with acceptable quality

KPMG

5.

Key takeaways



Key Takeaways

Start early, integrate CRA compliance into your product strategy, and treat it as a business enabler, not just a compliance burden

CRA is a product regulation

- Applies to products with digital elements across lifecycle
- Focus on secure-by-design and secure-by-default

Continuous compliance is required

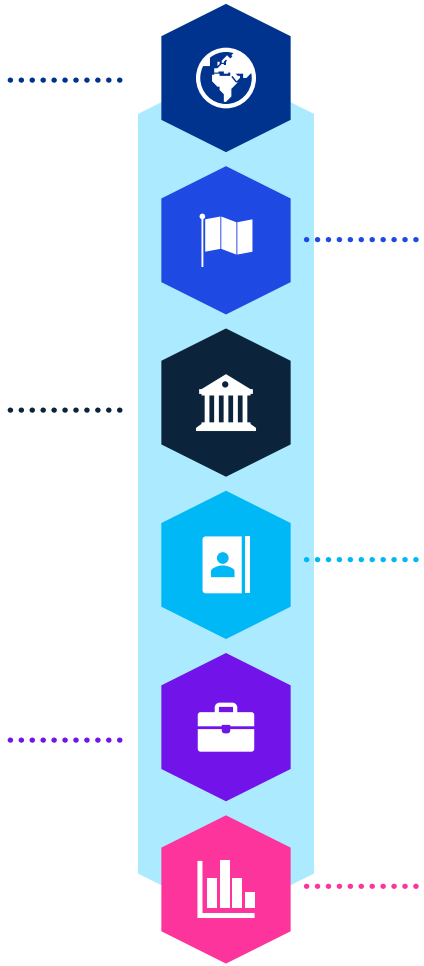
Not a one-time certification

Includes:

- Vulnerability handling
- Security updates
- Post-market monitoring

Enforcement is real and material

- Fines up to €15M / 2.5% global turnover
- Market withdrawal, recalls, bans



Accountability shifts to manufacturers

End-to-end responsibility:

- Design to development to lifecycle support
- Clear obligations also for importers & distributors

Documentation is a core control

Technical documentation, SBOM, risk files must be:

- Complete
- Up-to-date
- Audit-ready

Update your contracts to properly allocate CRA risks and responsibilities along the supply chain

Start now!

Building an operational model impact requires changes across:

- Product development (SDLC)
- Governance & accountability
- Incident & vulnerability management

kpmg.com