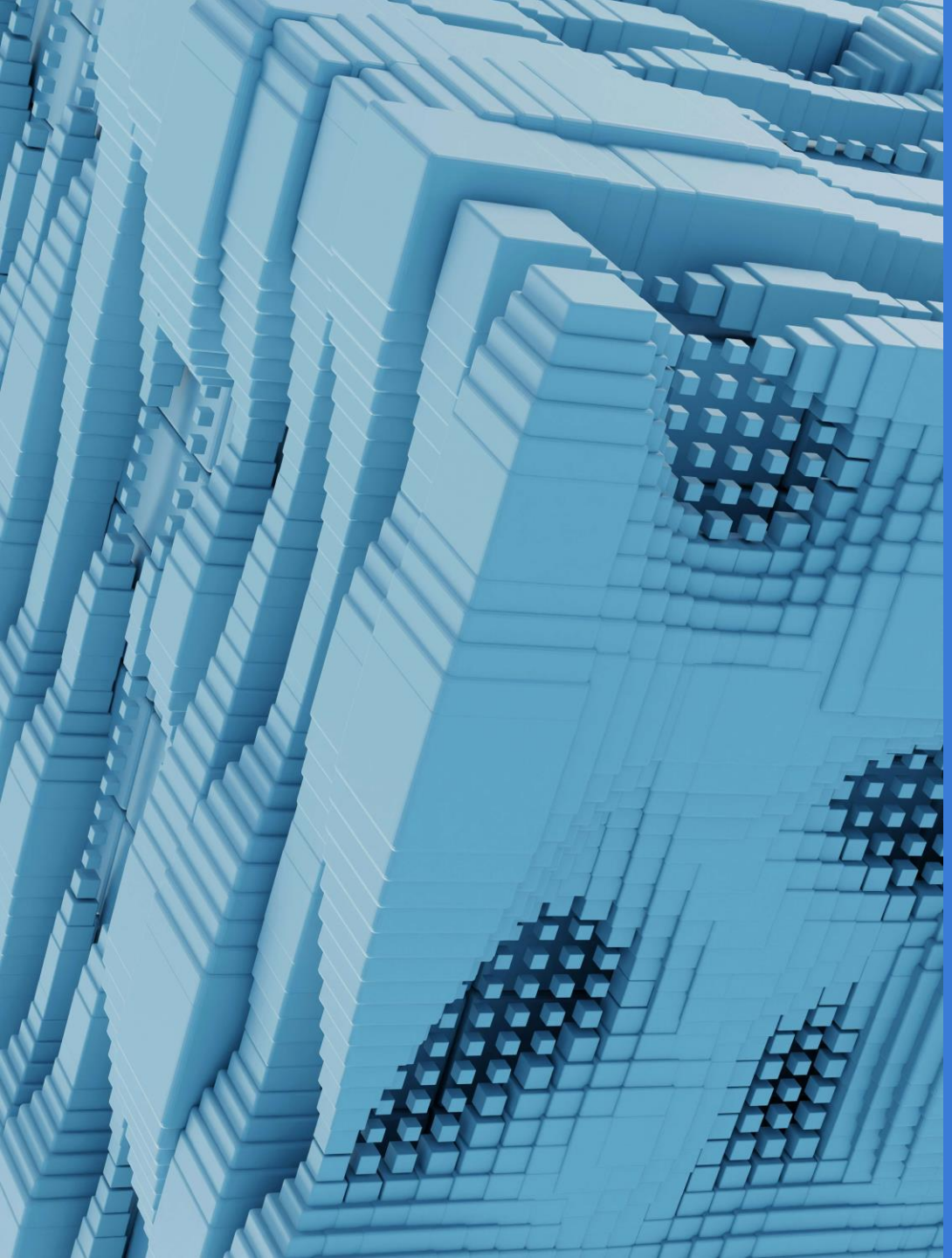


Getting ready for September 11

CRA Webinar

Nemko Digital

July 7, 2026

Nemko Digital

With you today

Gustavo Sánchez, Ph.D
AI Trust & Security Consultant
Nemko Digital

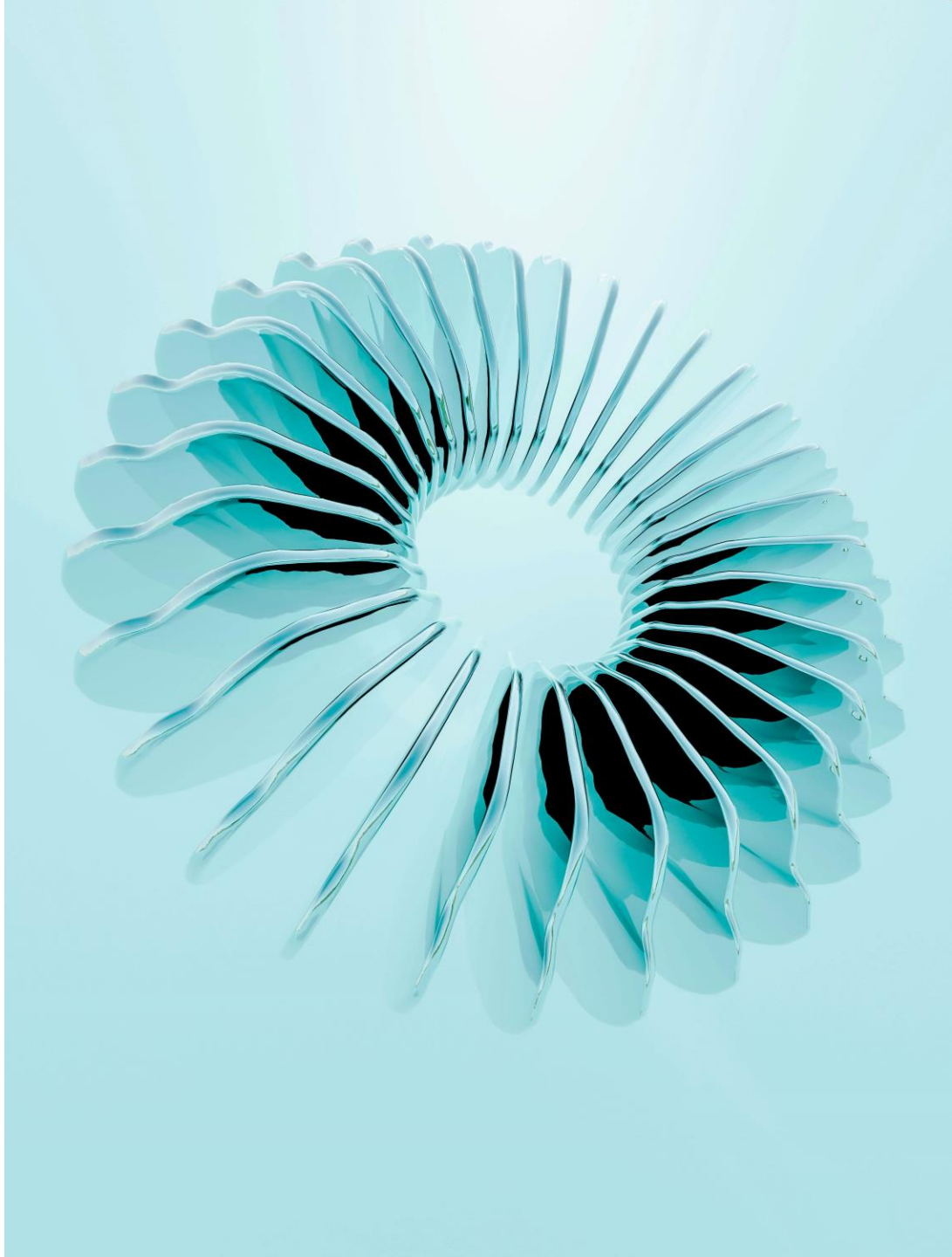
- **AI Trust Focus:** Trustworthy AI, regulatory compliance, and risk management under frameworks such as the EU AI Act and Cyber Resilience Act.
- **AI Security Researcher**: PhD in AI Security from the Karlsruhe Institute of Technology in Germany, with research focused on attacking and securing AI systems in critical infrastructure.
- **Bridging Research & Industry:** Experience collaborating with leading industry partners, translating cutting-edge research into practical, real-world security and assurance solutions.
- **International & Multidisciplinary Background:** Experience across Spain, Germany, the UK, and the Netherlands, with a strong applied background in AI, cybersecurity, and software engineering.

Pep van der Laan, Ph.D.
Digital Trust Expert
Nemko Digital

- **Scaling AI impact**: >10 years in realizing business value by scaling AI-powered digital products from initial proof-of-concept to enterprise-wide solutions.
- **Strategy advisory:** Extensive experience shaping the AI & Data transformation and architecture for global leaders and national champions across industries.
- **Capability building:** Led a team of 90 data engineers, AI developers, and data scientists through the transformation from the traditional consulting model and introducing modern delivery and development practices.
- **Growing Digital Trust:** Recognized for consistently bridging the gap between technology and the risk & legal stakeholders, building mutual understanding. Certified as ISO 27001 and ISO 42001 Lead Auditor.

CRA webinar: topics today

1. Introduction to Nemko Digital
2. CRA in brief – a quick overview
3. Meeting the September 11 deadline
4. Getting started
5. Q&A



Introduction Nemko Digital

Nemko: Compliance without Complexity

Strong heritage

1933 — Established by the Norwegian government as *Norges Elektriske Materiellkontroll*

1991 — Became independent self-owned private foundation

1992 - 2003 — Established offices and laboratories around the world

2020 — Launched Cybersecurity services

2024 — **Established *Nemko Digital* to consolidate AI Trust services**

Global reach & local presence

28 locations on 3 continents

Over **850** employees worldwide.

Offering services in more than **150** countries

Serving **7,000** customers across **80** countries.

In June 2025, Nemko signed a strategic partnership with KSA to shape the future of AI certification and trust in Korea and beyond

Proven track record

Roster of clients and services (not exhaustive)

SAMSUNG Panasonic LG JOTRON WÄRTSILÄ KÄRCHER

© 2026 All rights reserved by Nemko Digital: content and materials are not to be distributed or shared without prior permission.

What is top-of-mind for our clients?

We deliver Digital Trust through end-to-end compliance and advisory support, combining technical, regulatory, and process expertise.

Regulatory Compliance — Beyond AI

Technical Assurance / AI Testing

ISO Readiness
ISO 42001, ISO 27001…
— Beyond AI

AI Assurance Tools

Global Market Access — Beyond AI

Governance Maturity — Beyond AI

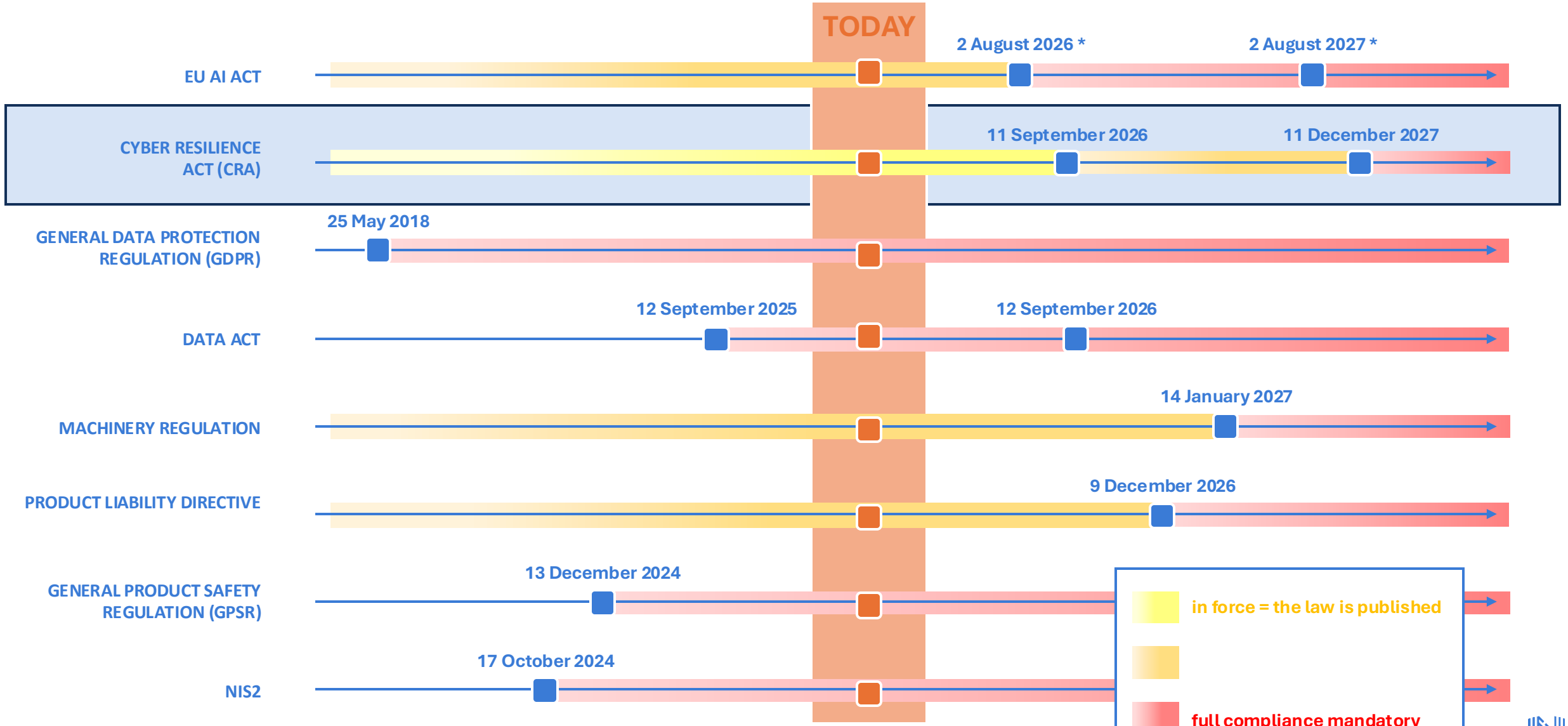
Nemko AI Trust Mark

Strategy and roadmaps — Beyond AI

© 2026 All rights reserved by Nemko Digital: content and materials are not to be distributed or shared without prior permission.

CRA in Brief

The CRA is part of a broader framework of digital EU regulations



© 2026 All rights reserved by Nemko Digital: content and materials are not to be distributed or shared without prior permission.

** Timeline subject to change due to proposed Digital Omnibus package*

CRA: Cyber Security for products

Fines up to
€ 15M or 2.5% of
global turnover

Objective of the CRA (EU) 2024/2847 is to **reduce cybersecurity vulnerabilities** for **products with digital elements** and create conditions allowing users to take cybersecurity into account when selecting and using products with digital elements

Key concepts:

- **Products with digital elements:** the CRA concerns both hardware and software
- **Remote data processing:** data processing at a distance is in scope of the CRA if it is essential for functioning
- **Security by design and default:** raising the bar for security of the product ‘as shipped’
- **Supply chain responsibility:** obligations cover the full digital supply chain, requiring manufacturers a.o. to report exploited vulnerabilities

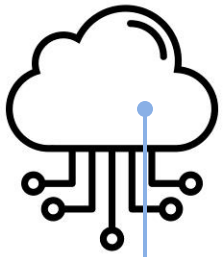
Key dates:

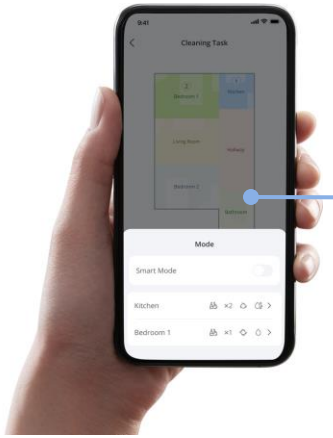
- **11 September 2026**: Mandatory vulnerability disclosure and incident reporting. Manufacturers must report within strict timelines.
- **11 December 2027:** Full compliance with CRA required. Non-compliant products cannot be sold in the EU.

The physical product and its digital elements throughout its lifetime

The **device and its software are treated as one product**, and any cloud or backend becomes part of that product if it's essential to how it works or stays secure.

Hardware product

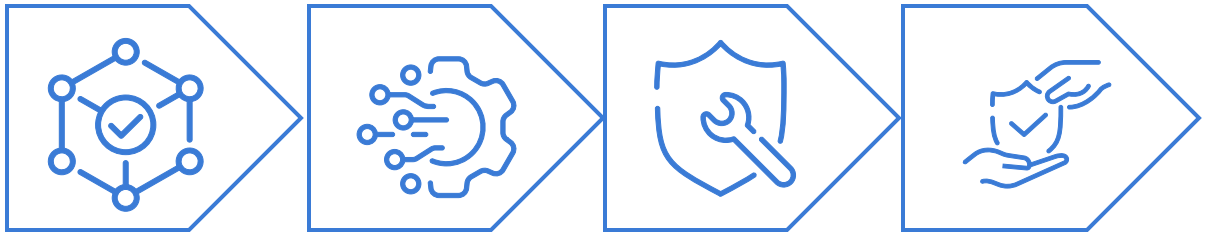




Supporting software

Remote Data Processing Solutions

The manufacturer can not limit its perspective to the product that is produced, but has responsibility for **components** and security throughout the **lifetime**



Design Sourcing Development Production

Links to other regulations

The CRA has important connections with the broader EU legislative framework

Radio Equipment Directive (RED)

- RED incudes radio, Electromagnetic compatibility (EMC), safety and cyber requirements
- RED cyber requirements are notably more limited than CRA requirements: additional effort is required to prove CRA compliance

AI Act

- High-risk AI systems that comply with CRA requirements have presumption of conformity on cybersecurity requirements as set out in the AI Act

Exceptions for specific product categories

Examples:

- Motor vehicles (EU) 2019/2144,
- Aviation (EU) 2018/1139 and
- Medical devices (EU) 2017/745&6

The way to Demonstrate conformity differs by product category

Critical products[1]

- Hardware devices with security boxes
- Smart meter gateways within smart metering systems
- Smartcards

Important Products[1]

Class I

- Identity management systems
- Browsers
- Password managers
- Malware protection software
- VPN products
- Network management systems
- SIEM systems
- Boot managers
- Key/certificate issuance software
- Network interfaces
- Operating systems
- Routers, modems and switches
- Microprocessors with security function
- Microcontrollers with security function
- ASIC & FPGA with security function
- Smart home GP VAs
- Smart home products with security functionalities
- Internet connected toys
- Personal wearables for health monitoring

Class II

- Hypervisors and container runtime systems
- Firewalls
- Tamper-resistant microprocessors
- Tamper-resistant microcontrollers

Default Products

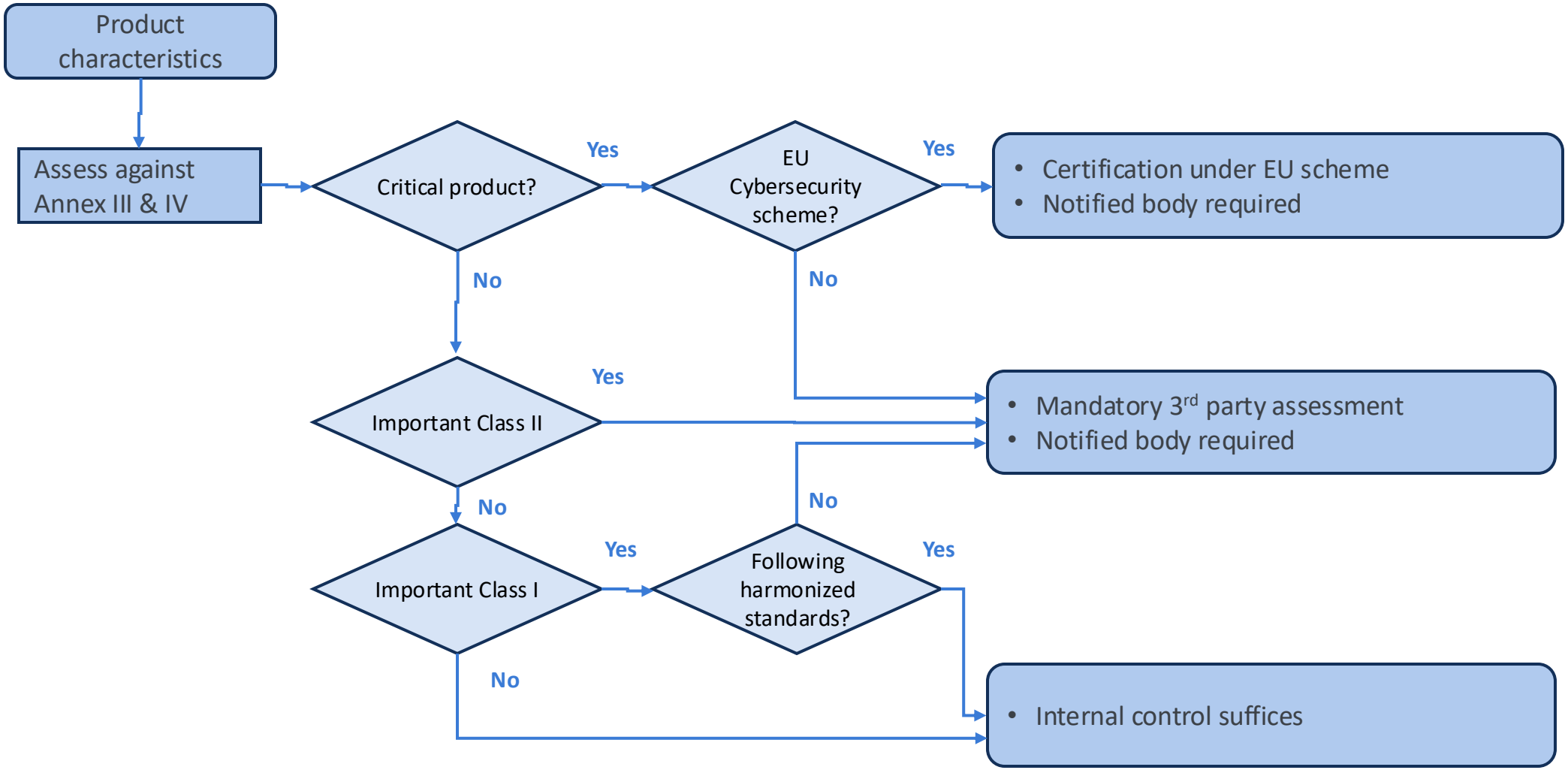
- All the rest

"Important products with digital elements as referred to in this Regulation should be understood as products which have **the core functionality** of a category of important products with digital elements"
CRA, recital 45

1. Implementing regulation (EU) 2025/2392 provides the official technical description of the categories of important and critical products with digital elements, as required by the CRA.

© 2026 All rights reserved by Nemko Digital: content and materials are not to be distributed or shared without prior permission.

The product category determines possible paths to conformity



Reporting obligations per September 11, 2026

- **Publicly disclose information about fixed vulnerabilities**
- **Policy on coordinated vulnerability disclosure (CVD)**
- **Provide a channel for reporting of vulnerabilities**
- **Contact information of the manufacturer**
- **Single point of contact for vulnerability disclosure and information on CVD**

Notably no explicit requirement on vulnerability handling.

However…. other regulations (e.g. General Product Safety Regulation and Machinery regulation) act as backstop

Full compliance per December 2027

Product

- Secure design, development, production (appropriate for level of cybersecurity risk)
- No known exploitable vulnerabilities
- Secure by default configuration
- Automatic security updates
- Protection from unauthorized access
- Protection of confidentiality of data
- Protection of integrity of data
- Data minimization
- Protection and mitigation of denial-of-service attacks
- Minimize the impact of the product (and connected devices) on other services
- Limited attack surface (including interfaces)
- Appropriate exploitation mitigation mechanisms and techniques
- Logging mechanism (with opt-out mechanism)
- Deletion and secure transfer of data and settings

Vulnerability handling

- Identify and document vulnerabilities and components (including SBOM)
- Provide security updates without delay
- Apply effective and regular tests and reviews of the security
- **Publicly disclose information about fixed vulnerabilities**
- **Policy on coordinated vulnerability disclosure (CVD)**
- **Provide a channel for reporting of vulnerabilities**
- Provide mechanisms to securely distribute automatic security updates
- Keep products updates for the support period (at least 5 years) free of charge

Information and communication

- **Contact information of the manufacturer**
- **Single point of contact for vulnerability disclosure and information on CVD**
- Unique identification of the product
- The intended purpose and security environment, essential functionalities and security properties
- Known or foreseeable circumstances that can lead to significant cybersecurity risks
- Where applicable: link to EU declaration of conformity
- The type of technical security support offered and the end-date of the support period
- Detailed security instructions and information (initial setup, changes, updates, data deletion, disabling updates, and integration)
- If publicly available: how to access the SBOM

© 2026 All rights reserved by Nemko Digital: content and materials are not to be distributed or shared without prior permission.

Quiz time!

How confident are you that you can meet the CRA requirements?

A. Just starting to learn what CRA is

B. Exploring what it takes to get compliant

C. Almost ready for September 11

D. Ahead of the game, working on December 2027 obligations

E. All set for full compliance

Meeting the September 11 deadline

What should be reported?

Actively Exploited Vulnerabilities:
Vulnerabilities in products with digital elements that are known to be currently exploited by a malicious actor.

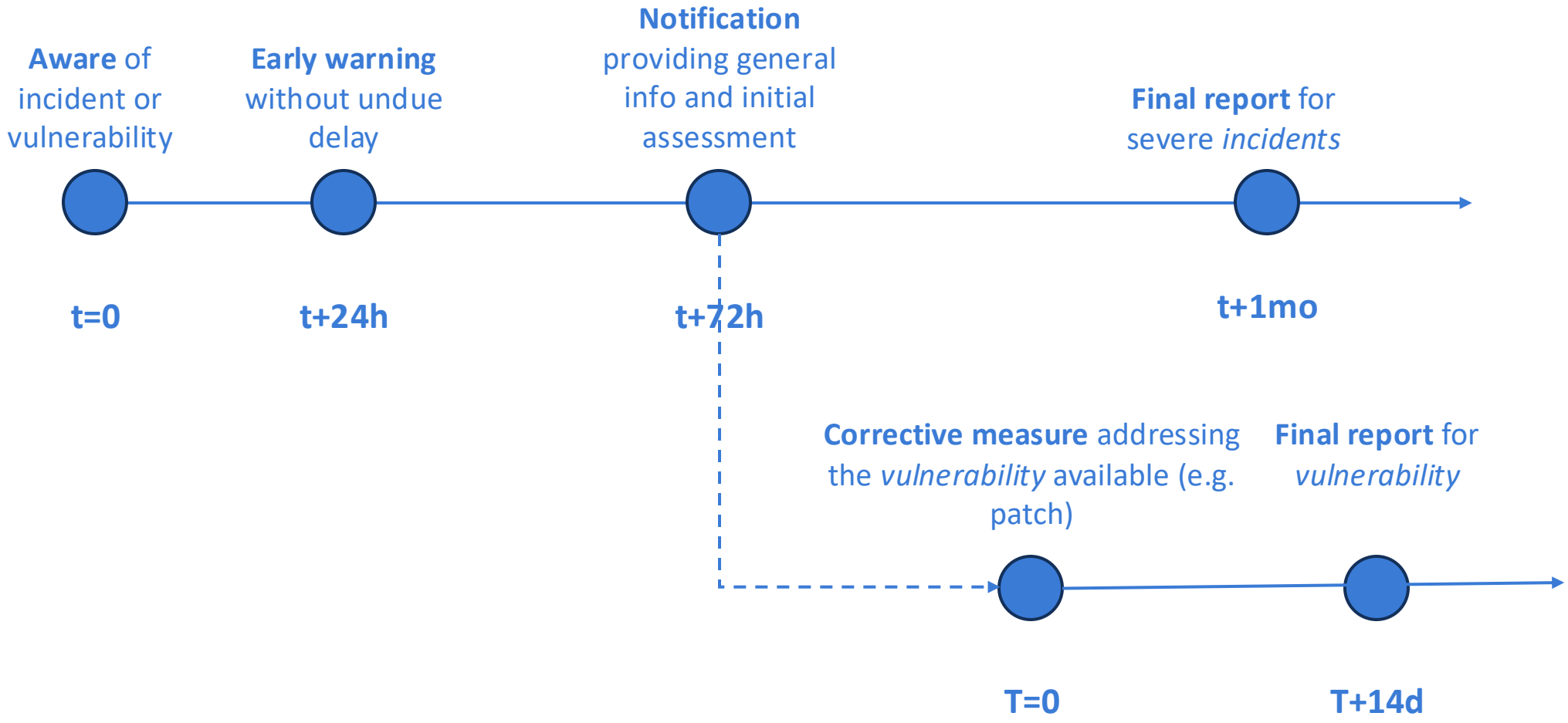
- Vulnerabilities in components only to be reported if these can be exploited in the product
- Zero-days only to be reported if exploited

Severe Incidents:
Incidents that have a severe impact on the security of the product with digital elements (e.g., compromising availability, authenticity, integrity, or confidentiality)

- Can negatively affect protective cyber capabilities, or
- Can lead to introduction or execution of malicious code

© 2026 All rights reserved by Nemko Digital: content and materials are not to be distributed or shared without prior permission.

Reporting obligations in detail



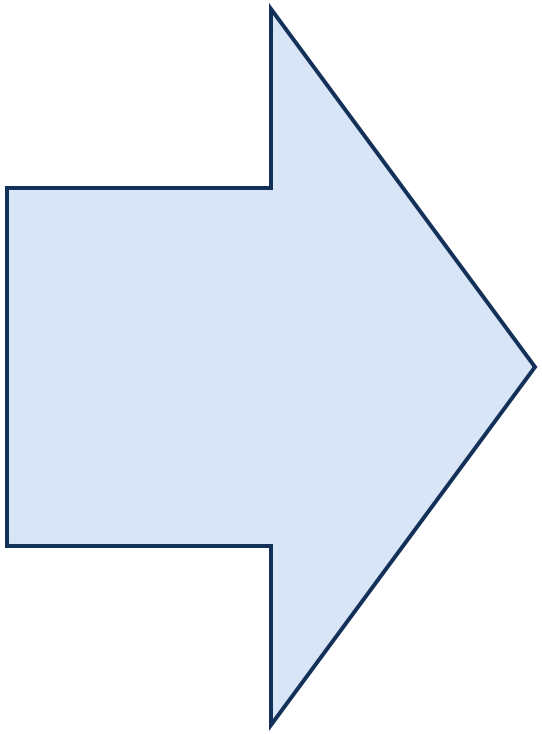
© 2026 All rights reserved by Nemko Digital: content and materials are not to be distributed or shared without prior permission.

Vulnerability and Incident Documentation

Traceable

Testable

Treatable

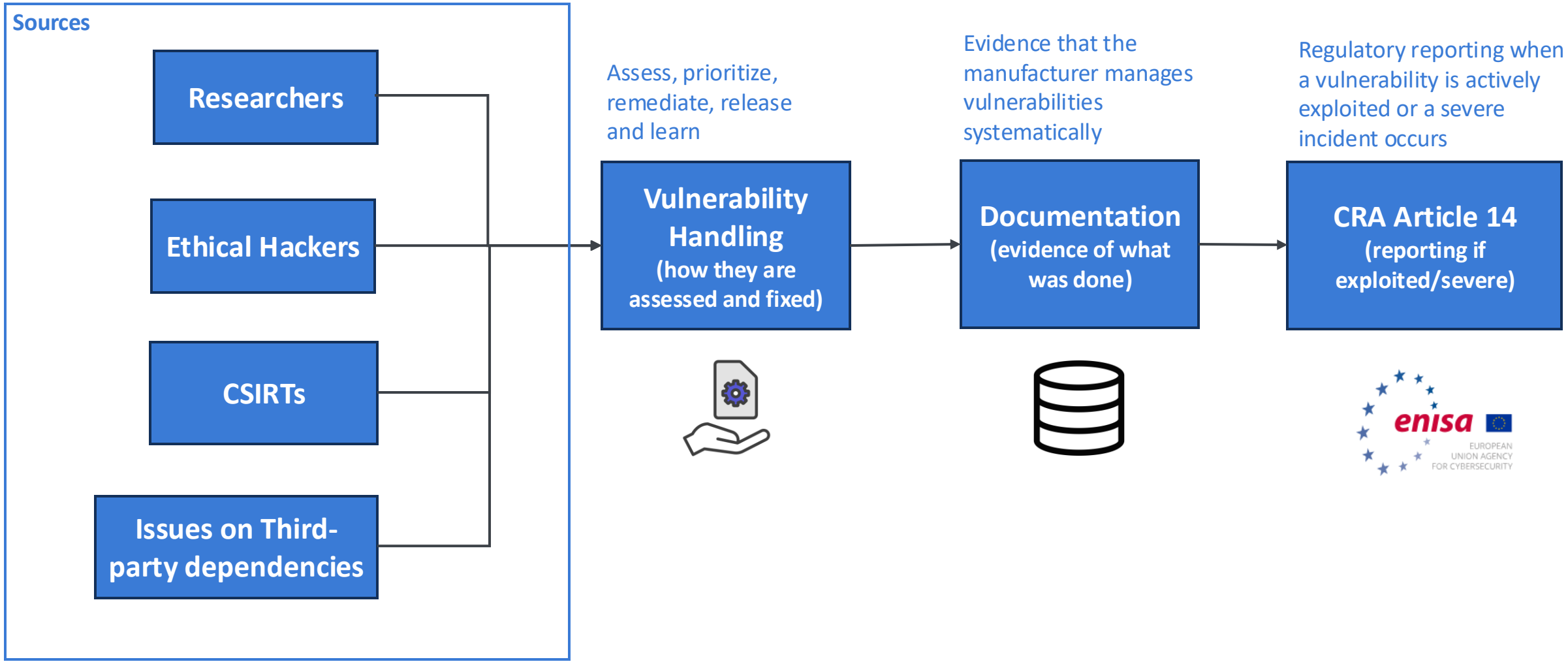


Mandatory fields for September 11th 2026 Deadline
ID
Type
Status
Product
Version
Description
Severity
Risk Level
Exploitation Status
Mitigation
Update Released?
Discovery Date
Fix Date
Root Cause
…

More to be added towards December 2027

Vulnerabilities: CRA Context

CVD = Structure for external parties to report vulnerabilities



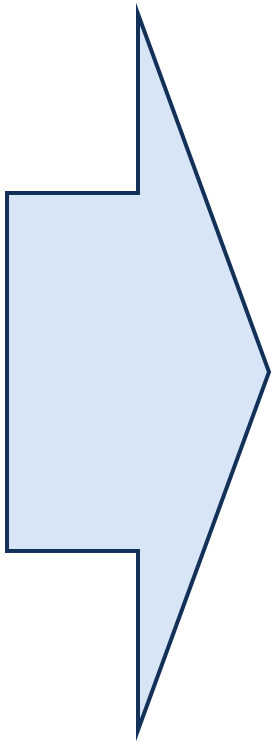
© 2026 All rights reserved by Nemko Digital: content and materials are not to be distributed or shared without prior permission.

Requirements on Vulnerability Disclosure Policy and Process

Accessible

Confidential

Acknowledged



Requirements
Reporter can submit without identity; no mandatory personal fields
Web form available on public website, no login required
Form collects description, product, steps, impact
Each submission generates an ID for traceability
Reporter receives confirmation within defined timeframe
Use TLS for form; optionally PGP/email for sensitive data
Access restricted to authorized personnel only
Submissions must be actively monitored and processed
Form captures product name/version/component
Data must allow validation, reproducibility, severity assessment
Provide multiple accessible communication methods
Enable follow-up communication with reporter
…

Where and how to report?

- Use the CRA **Single Reporting Platform** (SRP)
- Submission goes to **CSIRT** (country of main establishment) and is simultaneously accessible to **ENISA**

- The EU Agency for cybersecurity (ENISA) awarded the contract for the development of the **Single Reporting Platform (SRP)** to a trilateral consortium.
- The platform is scheduled to be operational by **11 September 2026**. A testing period is expected to take place before this date.
- Specific manual and instructions will be provided by ENISA in the course of **June 2026** according to ENISA's Q&A; this seems to be delayed.

© 2026 All rights reserved by Nemko Digital: content and materials are not to be distributed or shared without prior permission.

What are the capabilities you need to fulfill the reporting obligations?

Detection capability

- Capability to detect exploited vulnerabilities
- and severe incidents

Internal classification rules

- Is that an exploited vulnerability?
- A severe incident?

Reporting workflow

- Must assign who decides
- and who submits reports

Responsible roles

- Detection → classification → 24h alert → 72h report → final report
- Must support informing users and providing mitigations

Reporting interface and recordkeeping

- Access to SRP and ability to create structured reports
- Must collect timestamps, submit content and follow ups

Manufacturer MUST inform impacted users

- Share vulnerability/incident and mitigation instructions

© 2026 All rights reserved by Nemko Digital: content and materials are not to be distributed or shared without prior permission.

Getting started

Overview of key CRA requirements

The Cyber Resilience Act puts requirements both on the **products** with digital elements and on the processes that **manufacturers** of these products have in place

Product requirements

- Secure by default and design
- Security updates
- Data minimization
- Resilience (after incidents)
- User information
- Data transfer

Process requirements

- Vulnerability risk assessment
- Testing and review
- Information sharing (vulnerabilities and updates)
- Secure dissemination of security updates

What this asks from organizations:

- Integrating **product security** with **organizational governance**
- Moving from ad-hoc controls to **repeatable, documented processes**
- Linking **engineering**, **compliance**, and **operational security**
- Embedding continuous **vulnerability management**
- Connecting **product lifecycle** with corporate **risk frameworks**

Common challenges we see at clients

Unclarity about standards

- Lack of harmonized standards yet
- Relationships with RED, NIS2, etc.

Decentralized processes

- Independently operating product teams
- Fragmented ownership across departments

Limited visibility on software components

- SBOM gaps and dependency management
- Supplier risk and OSS governance

Resource and capability constraints

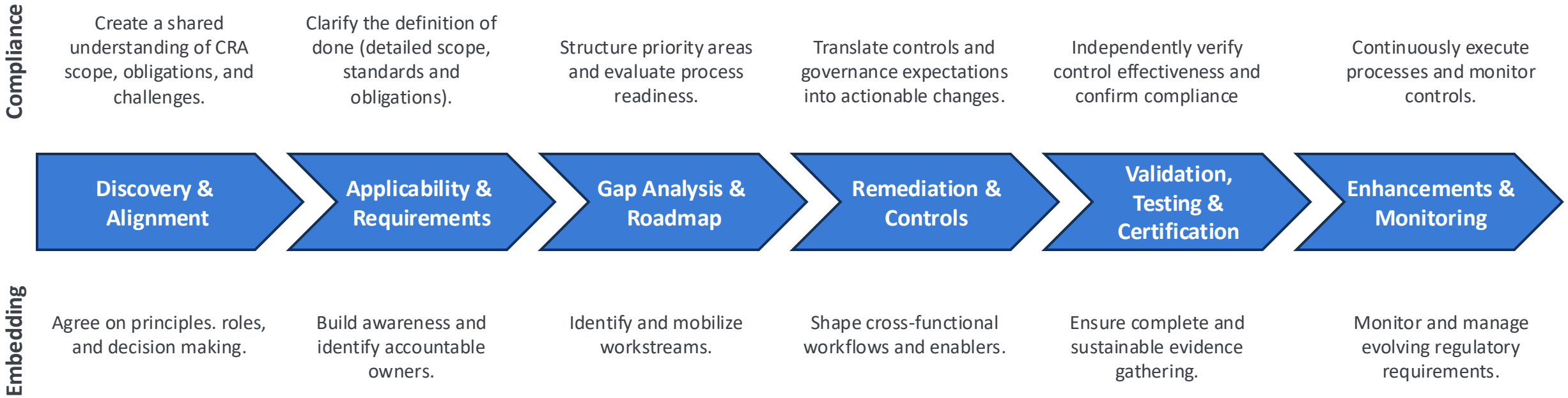
- Limited CRA expertise
- Competing priorities in product roadmaps

Organizational readiness

- Proactive security design over reactive fixes
- X-functional accountability and collaboration

Nemko’s CRA readiness approach

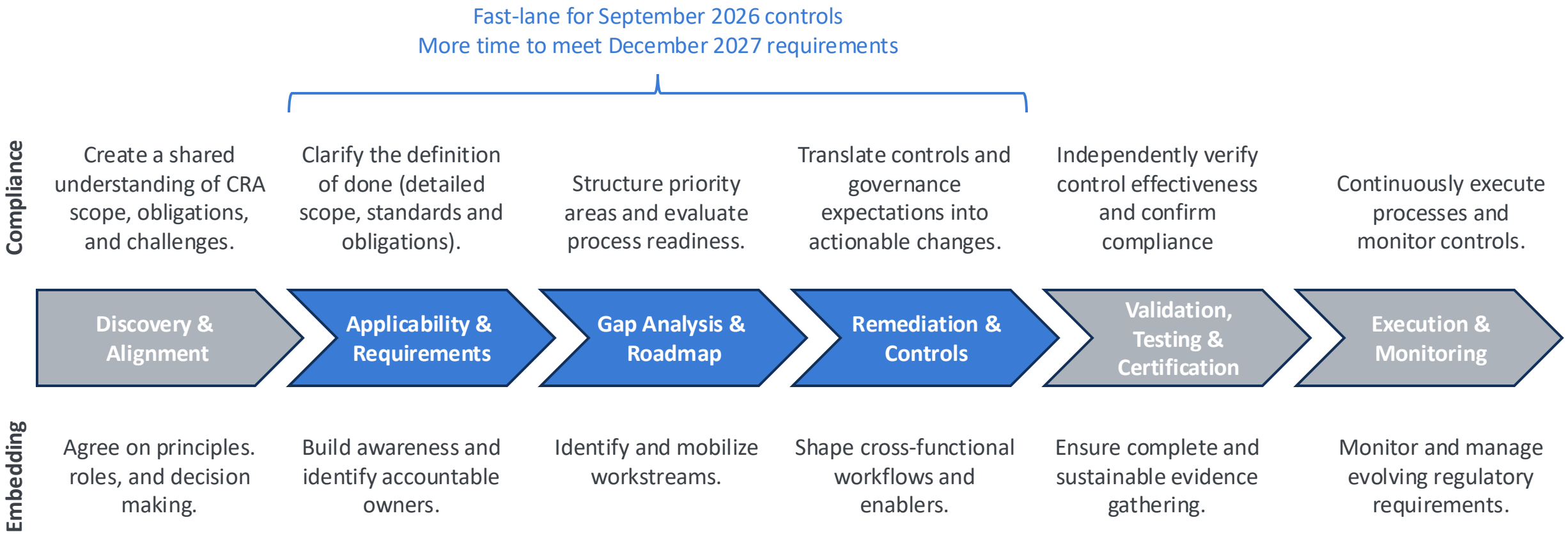
A phased approach to interpret, remediate, validate, and continuously manage regulatory obligations.



© 2026 All rights reserved by Nemko Digital: content and materials are not to be distributed or shared without prior permission.

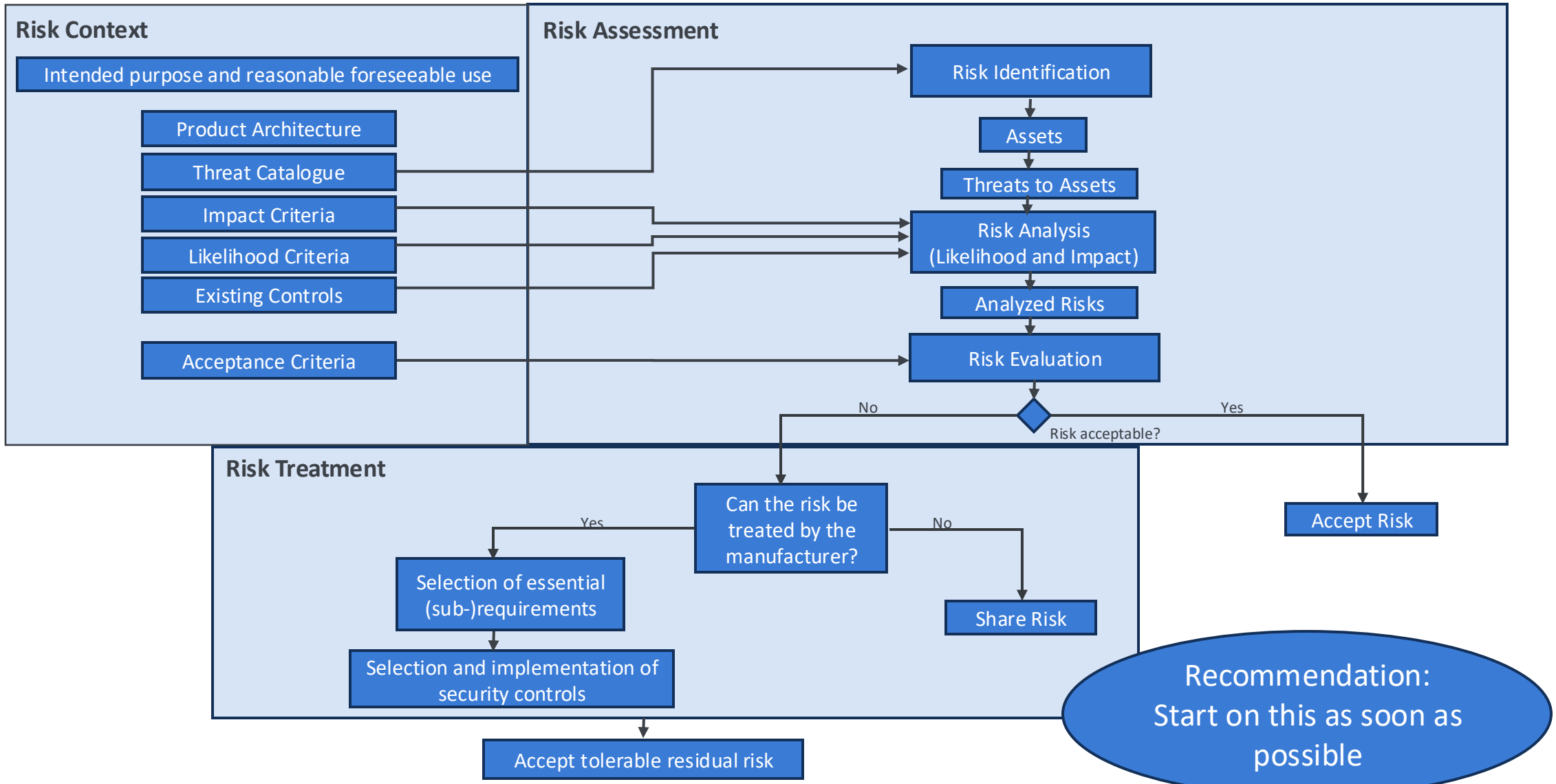
Nemko’s CRA readiness approach

Nemko offers a phased approach to interpret, remediate, validate, and continuously manage regulatory obligations.



© 2026 All rights reserved by Nemko Digital: content and materials are not to be distributed or shared without prior permission.

Note: a cyber risk assessment is foundational for compliance



© 2026 All rights reserved by Nemko Digital: content and materials are not to be distributed or shared without prior permission.

Nemko Digital

Call with our CRA experts now!

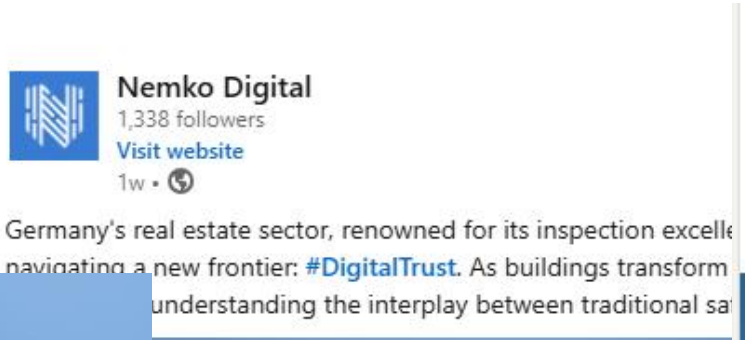
Don’t wait till April for the next step

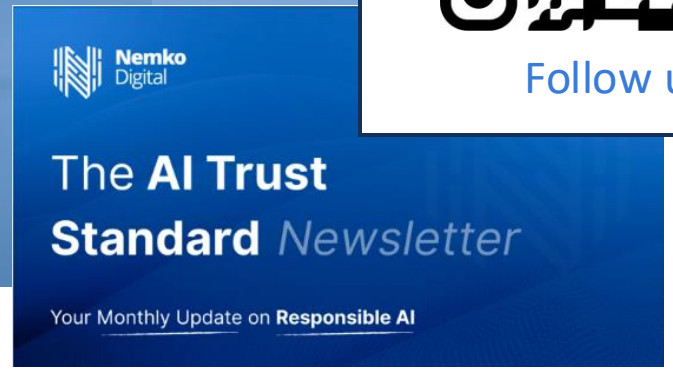
- Open to Webinar Participants
- Complete Application Form
- Share topic you want to talk about

https://digital.nemko.com/cra-expert-call

Scan to apply

Stay updated!





Follow us

© 2026 All rights reserved by Nemko Digital: content and materials are not to be distributed or shared without prior permission.

Nemko
Digital