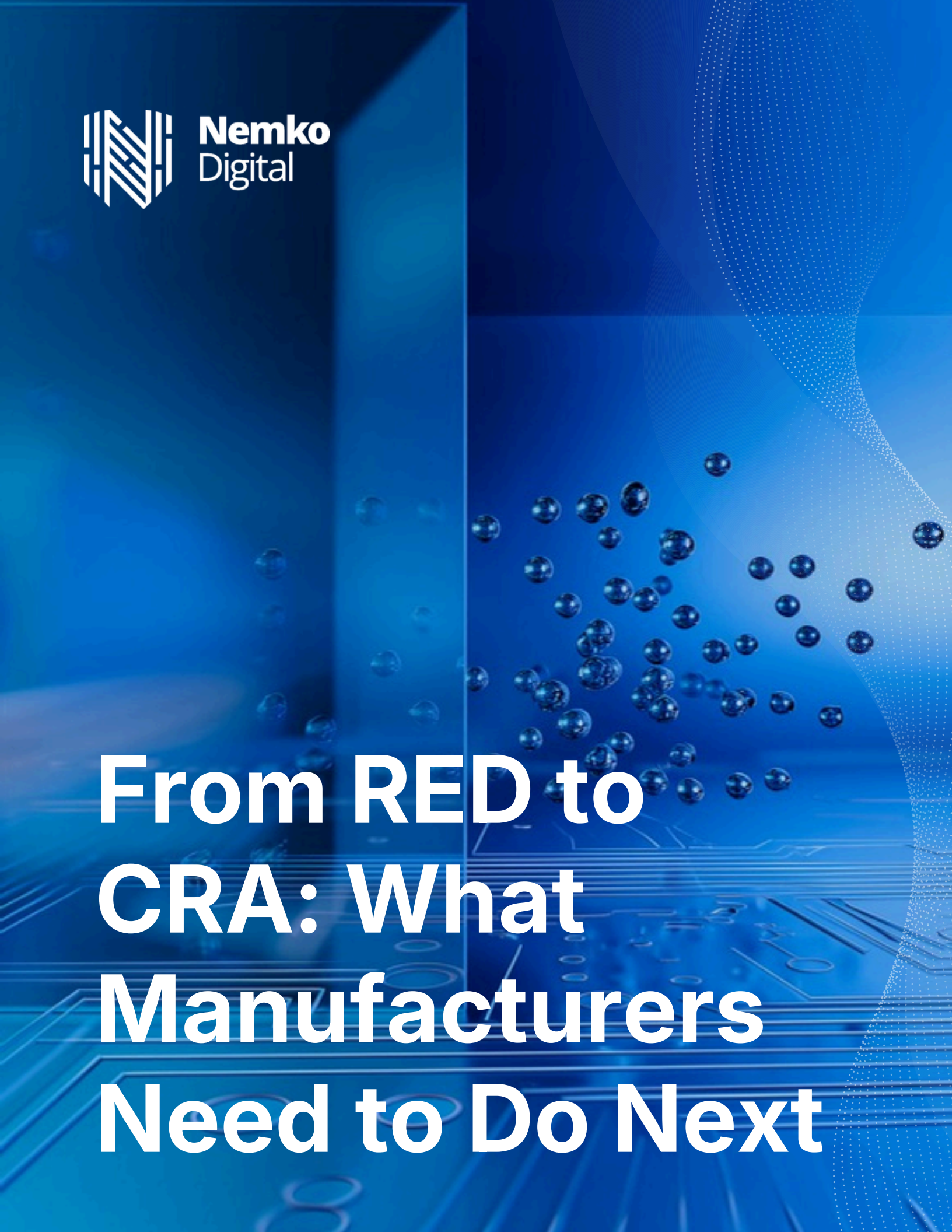


From RED to CRA: What Manufacturers Need to Do Next

As the EU Cyber Resilience Act (CRA) moves toward full applicability, many of our clients (especially As the EU Cyber Resilience Act (CRA) moves toward full applicability, many of our clients (especially those already aligned with the Radio Equipment Directive (RED) and the EN18031 standard for internet radio equipment) are asking a practical question:

How much of this work can we reuse, and what really changes?

This article highlights key areas in the transition from RED to CRA, understanding the role of standards, and handling products with critical components.

The evolving cyber threat and regulatory landscape

The original Radio Equipment Directive (EU directive 2014/53/EU) was passed in 2014 and became fully applicable in 2017. This was is a world that was much different from today. Cyber threats have become more aggressive: faster, more sophisticated, and more ruthless. And a brief glance at the capabilities of AI (e.g. Anthropic's Project Glasswing) demonstrate that this development is not slowing down anytime soon.

In 2022, RED Cyber ((EU) 2022/30) was passed as a delegated reguation, effective 1 August 2024, introducing cybersecurity obligations for internet-connected radio devices. In particular:

- The equipment must not harm networks or misuse resources.
- The equipment must safeguard personal data and privacy.
- The equipment must be protected against fraud.

In 2025, the harmonized standard EN18031 was published, providing a basis for presumption of conformity (with restrictions). Over the last few years, manufacturers have invested significantly in proving conformity.

In the meantime, the Cyber Resilience Act ((EU) 2024/2847) was passed, putting forward requirements for products with digital elements; leaving many manufacturers wondering how to pursue an incremental approach to conformity.

From RED (EN 18031) to CRA: What Changes?

Manufacturers that have already implemented EN 18031 under RED are in a strong starting position. The RED Delegated Regulation (2022/30) introduced cybersecurity requirements focused on radio equipment.

The CRA builds on similar principles, but significantly broadens scope of applicability and depth of obligations.

What you can reuse

If you are RED-compliant using EN 18031, you already have:

- A risk-based cybersecurity approach
- Product-level security requirements embedded by design
- A technical documentation and conformity assessment processes
- Some vulnerability considerations
- Some supply chain considerations

TThese elements provide a good start towards CRA “essential cybersecurity requirements” and evidence on these points will contribute to CRA compliance on these elements, but will not be sufficient.

Disclaimer: as of this writing (May 2026), there are no harmonized standards for CRA yet and notified bodies have not yet been appointed.



What you still need to add

In several ways, the CRA goes beyond RED Cyber:

1. **Lifecycle responsibility:** Where RED is largely focused on compliance at market placement, CRA introduces additional continuous obligations, including vulnerability handling and security updates throughout the expected product lifetime.
2. **Vulnerability management & reporting:** Mandatory policies and processes for vulnerability handling (intake, triage, disclosure) and reporting in CRA go beyond what is expected under RED.
3. **Supply chain depth:** The CRA elevates the RED requirement to the obligation to an appropriate level of due diligence based on a well maintained machine readablesoftware bill of materials (SBOM).
4. **Secure development practices:** Where RED puts forward specific requirements that affect specific elements of the Software Development Lifecycle (SDLC), CRA requires secure practices across.
5. **Documentation:** When it comes to component transparency and dependency management, CRA is much more explicit than RED.

RED compliance gives you a strong technical foundation, but CRA requires additional operationalization, lifecycle governance, and supply chain maturity.

Navigating emerging standards

Understanding how standards will work under CRA is critical for planning. Various standards are currently in different stages of the development process. Nonetheless it is valuable to provide an early perspective on how these standards will work.

Horizontal and vertical standards

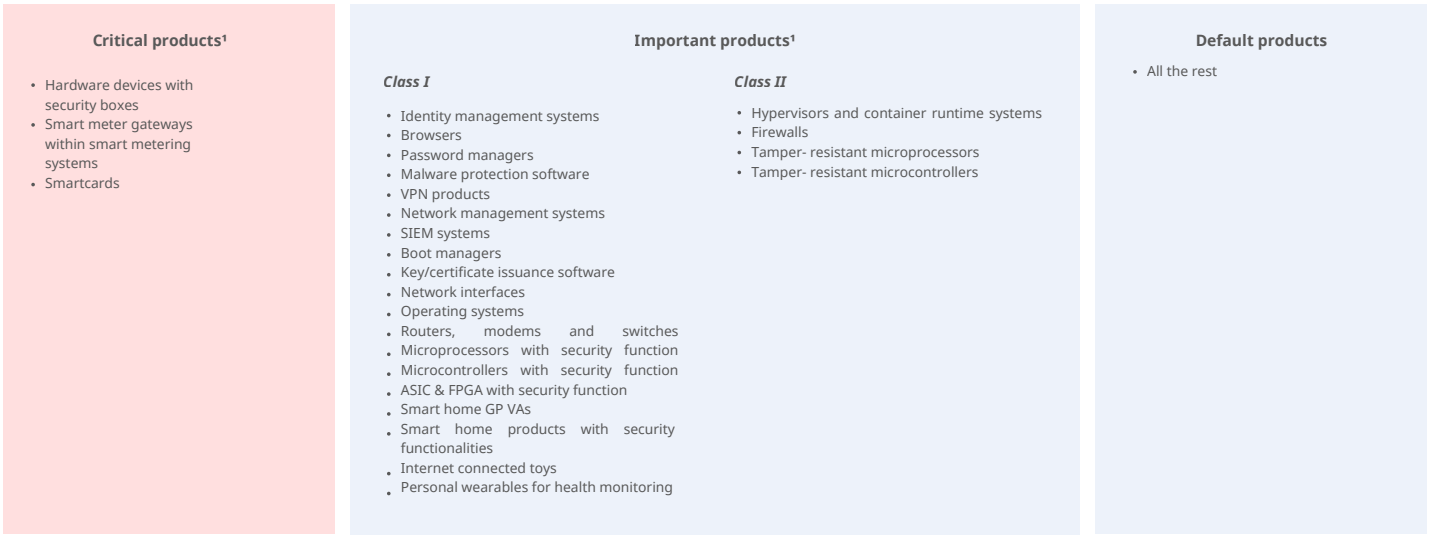
Horizontal standards are cross-sector standards that apply broadly across product categories. Horizontal standards provide a baseline of reusable building blocks to demonstrate compliance with CRA essential requirements. Elements like a secure SDLC, vulnerability management, and encryption standards will (likely) be covered by horizontal standards.

Vertical standards are product- or sector-specific standards. Vertical standards translate CRA requirements into context-specific implementations, addressing specific risks in certain product classes. Draft standards for various products like smart home virtual assistants, browsers, and network management systems are currently already available.

Where horizontal standards cover primarily organizational and process maturity, vertical standards provide expectations for product-specific compliance. Together they provide a definition of done for companies seeking to prove conformity.

Products and components

The way to Demonstrate conformity differs by product category



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.

"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

Figure 1: CRA product categories differ by conformity route. Manufacturers should assess whether the product's core functionality places it in the default, important, or critical category before defining the evidence and conformity path.

- Default products
- Important products Class I
- Importanct products Class II
- Critical products

The product category reflects the importance of the product for cyber security. for example: smartcards are Critical, passwordmanagers Important class I, and consumer electronics typically Default.

A common misconception is: "If my product contains a critical component, my product automatically becomes critical." This is not how CRA works. What matters is the core functionality of the product: Does the product itself perform a security-sensitive role? Is it widely deployed in a high-impact environment?

An operating system is a Important Class I product. However, a smartphone containing an operating system (Android, iOS) does not have operating system as its core functionality and is considered Default product.

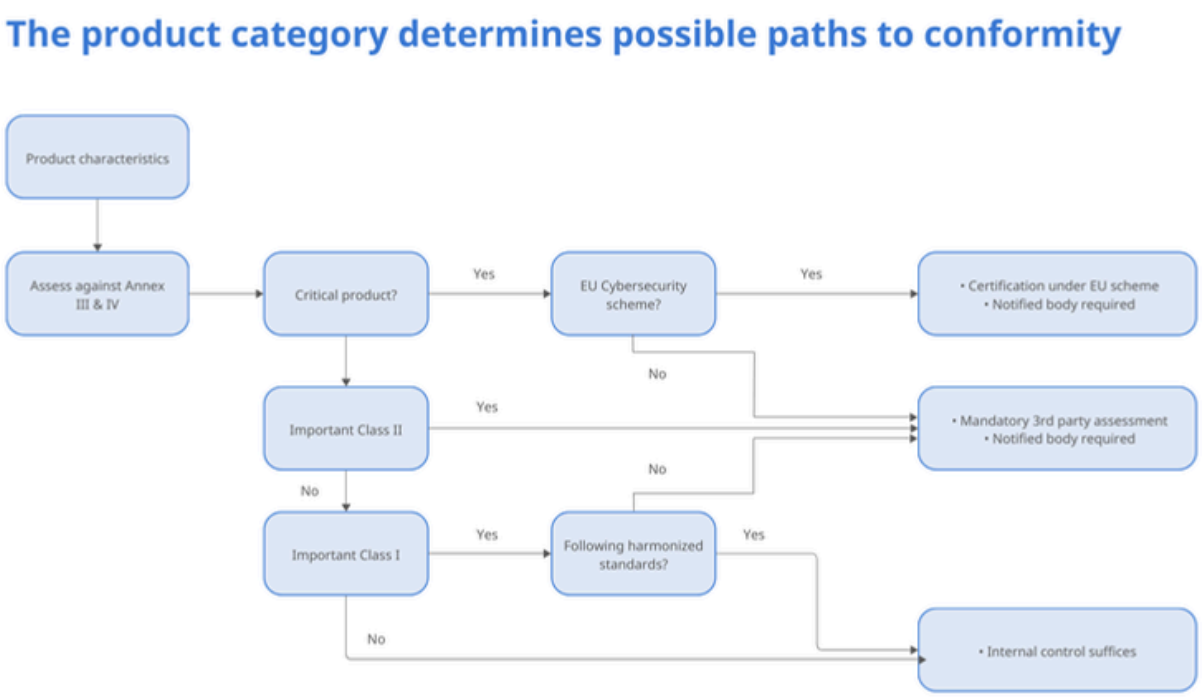


Figure 2: Product category determines the route to conformity. Critical and Important Class II products may require third-party involvement, while other products may follow internal control where the relevant conditions are met.

Your next move

With deadlines for CRA compliance fast approaching, it is important to create clarity on where you stand and what the essential steps to take are, towards conformity with the September 2026 and December 2027 deadlines.

Do you need support, or do you want to validate your thinking? Reach out to our experts!

About the author



dr. Pepijn van der Laan

Global Technical Director, AI Governance | Nemko Group
With two decades of experience at the intersection of AI, strategy, and compliance, Pep has led groundbreaking work in AI tooling, model risk governance, and GenAI deployment. He has advised multinational organizations on scaling trustworthy AI—from procurement chatbots to enterprise-wide model oversight frameworks.



Daniel Breive Havre

Service Delivery Manager for Nemko Cyber Security Scandinavia
Experience with a range of different cybersecurity schemes and evaluation. Assessing products (both Software and hardware) and systems on a consumer grade basis, industrial and critical infrastructure related. Daniel has been working with everything from startup companies to large industry leading companies, ensuring cyber security compliance and making the world a safer place from a cyber perspective.

Nemko Digital