Nemko Digital

CASE STUDY

CRA Readiness at Scale

How a Global Leader in Healthcare Education Products Classified, Assessed, and De-Risked 70+ Products Under the EU Cyber Resilience Act

Executive summary

As the EU Cyber Resilience Act (CRA) shifts cybersecurity from a best practice to a legal precondition for market access, manufacturers of connected products face a narrow window to classify, assess, and remediate their portfolios before enforcement begins. This case study shows how a **global leader in healthcare education and resuscitation training** embarked on that journey. The company, whose mission is to help save one million lives every year by 2030 through medical manikins, simulation software, and connected medical devices, partnered with Nemko Digital to bring CRA readiness to its entire connected product portfolio.

Within two months' time from project kick-off to final delivery, Nemko Digital **classified more than 70 products against the CRA's risk categories**, conducted a structured gap analysis across process, governance, and technical documentation, and identified a path to reduce both compliance cost and time to market. Where products had initially been assumed to fall under the higher-scrutiny Class I – Important category, closer analysis of functional scope allowed several to be justifiably re-classified as Default, **easing the compliance burden without compromising due diligence**.

The result is a documented, defensible classification for the full portfolio and a **clear, prioritized roadmap covering vulnerability handling, incident reporting, cyber risk assessment, supply chain risk management, and substantial modification determination** which comprise the core pillars of CRA compliance. Beyond the immediate deliverable, the engagement gave the organization a **repeatable methodology it can apply as new products** are developed and as the CRA's harmonized standards and enforcement guidance continue to mature.

Section 01

Situation

01

The Client is a global manufacturer of medical training manikins, simulation software, and connected medical devices used by hospitals, universities, and first responders around the world. Its products sit at the intersection of medical device regulation and, increasingly, cybersecurity regulation: a growing share of the portfolio now includes network-connected components, embedded software, and data-handling functionality that fall within the scope of the EU Cyber Resilience Act.

With the CRA introducing binding obligations for products with digital elements, the Client needed to understand, product by product, where it stood. The portfolio spanned dozens of product lines developed over a decade, each with its own architecture, connectivity profile, documentation maturity and product team silos, but no consolidated view of CRA applicability or risk classification existed.

The Client engaged Nemko Digital to classify its connected product portfolio under the CRA, assess each product's current state of compliance readiness, and define a practical, prioritized path to conformity, all without slowing the organization's broader mission of expanding access to life-saving training and simulation technology.

Section 02

02

Challenges

The scale and diversity of the portfolio, combined with the CRA's still-maturing implementing guidance for a single level online platform, created several distinct challenges:

Portfolio-wide scope, no consolidated classification

With more than 70 distinct products across manikins, software, and connected devices, the Client had no unified inventory linking each product to its CRA risk category, applicable obligations, or conformity pathway.

Risk of over-classification

Several products had initially been presumed to fall under Class I – Important, the CRA's higher-scrutiny category, without a rigorous functional-scope analysis to confirm whether that classification was warranted. This created a risk of over-classification, unnecessary conformity assessment burden, and inflated compliance cost.

Supply chain visibility

As a connected-device manufacturer, the Client needed to determine the extent to which its supply chain (including component suppliers, embedded software providers, and contract manufacturers) introduced CRA-relevant risk that had not previously been systematically assessed.

Fragmented documentation and governance

Product documentation, security processes, and governance structures had developed organically over time and were not organized in a way that could be readily mapped to CRA requirements, making it difficult to identify gaps or demonstrate readiness to regulators.

Undefined substantial modification criteria

The CRA introduces specific triggers, such as substantial modification, that reset or alter conformity obligations. Without a clear internal definition of what constitutes a substantial modification for its own products, the Client risked inconsistent decisions across product teams.

Section 03

03

Our Approach & Solution

Nemko Digital structured the engagement in two phases: a rapid, portfolio-wide classification exercise, followed by a targeted gap analysis for each classified product.

Phase 1: Portfolio classification

Working closely with the Client's product, compliance and technical development teams, Nemko Digital reviewed more than 70 products against the CRA's classification criteria within one month. Each product was evaluated based on its functional scope, connectivity, data handling, and intended use, rather than by category assumption alone.

This close, function-first analysis allowed several products that had initially been treated as Class I – Important to be justifiably re-classified as Default classification once their actual functional scope was examined against the CRA's criteria. This reduced the number of products subject to the more demanding conformity assessment route, lowering both compliance cost and time to market while preserving a defensible, evidence-based classification rationale for every product in the portfolio.

Section 03

03

Phase 2: Structured gap analysis

For each classified product, Nemko Digital conducted a gap analysis structured around three consistent lenses:

- **Process / Policy.** Identifying additional information and documentation required to meet CRA obligations, including vulnerability handling procedures, incident reporting mechanisms, and cyber risk assessment records.
- **Governance.** Assessing the organizational people, processes, and workflows needed to ensure compliance is not a one-time exercise but a sustained capability as products evolve and new CRA guidance emerges.
- **Technical / Product Documentation.** Reviewing existing technical and product documentation where applicable, to determine how much could be reused or adapted to satisfy CRA documentation requirements versus what needed to be created from scratch.

Across both phases, the gap analysis was anchored around the CRA's core compliance pillars: **vulnerability handling, incident reporting, cyber risk assessment, supply chain risk management, and substantial modification determination**.

> *Cyber resilience is becoming as fundamental to medical technology as clinical safety. Helping a manufacturer whose mission is to save a million lives a year build that resilience into its products is exactly the kind of impact we set out to have.*

Section 04

Value Delivered

04

The engagement gave the Client a complete, defensible view of CRA applicability across its portfolio and a practical foundation for ongoing compliance.

70+

Products classified under the CRA

2 months

Time to complete portfolio-wide classification & gap analysis

3

Gap analysis lenses applied per product: policy/process, governance, technical documentation

Reduced compliance cost and complexity

By analyzing functional scope rather than relying on initial assumptions, several products were justifiably moved from Class I: Important to Default classification, reducing conformity assessment burden and associated cost across the portfolio.

A simplified, defensible pathway to conformity

Every product now has a documented, evidence-based CRA classification and a corresponding gap analysis, giving the organization a clear, prioritized view of what remains to be done ahead of enforcement deadlines.

Section 04

04

Targeted, risk-based remediation

With gaps assessed across process, governance, and technical documentation, the Client can direct remediation effort to where it matters most, rather than pursuing uniform, resource-intensive changes across the entire portfolio.

A reusable framework for future products

The classification methodology and gap analysis framework are designed to be reused as new products are developed, providing a repeatable model for embedding CRA readiness into the product development lifecycle rather than treating it as a one-time exercise.

Stronger internal alignment

With clearer, function-based classification and defined substantial modification criteria, product teams can make design and connectivity decisions with a better understanding of their regulatory consequences, reducing the risk of unplanned re-classification later in the product lifecycle.

As the Cyber Resilience Act moves from published regulation to active enforcement, the ability to demonstrate a rigorous, well-documented classification and compliance pathway is expected to become a baseline expectation for manufacturers of connected medical technology, a factor in continued EU market access, and most importantly, customer trust.


Nemko
Digital