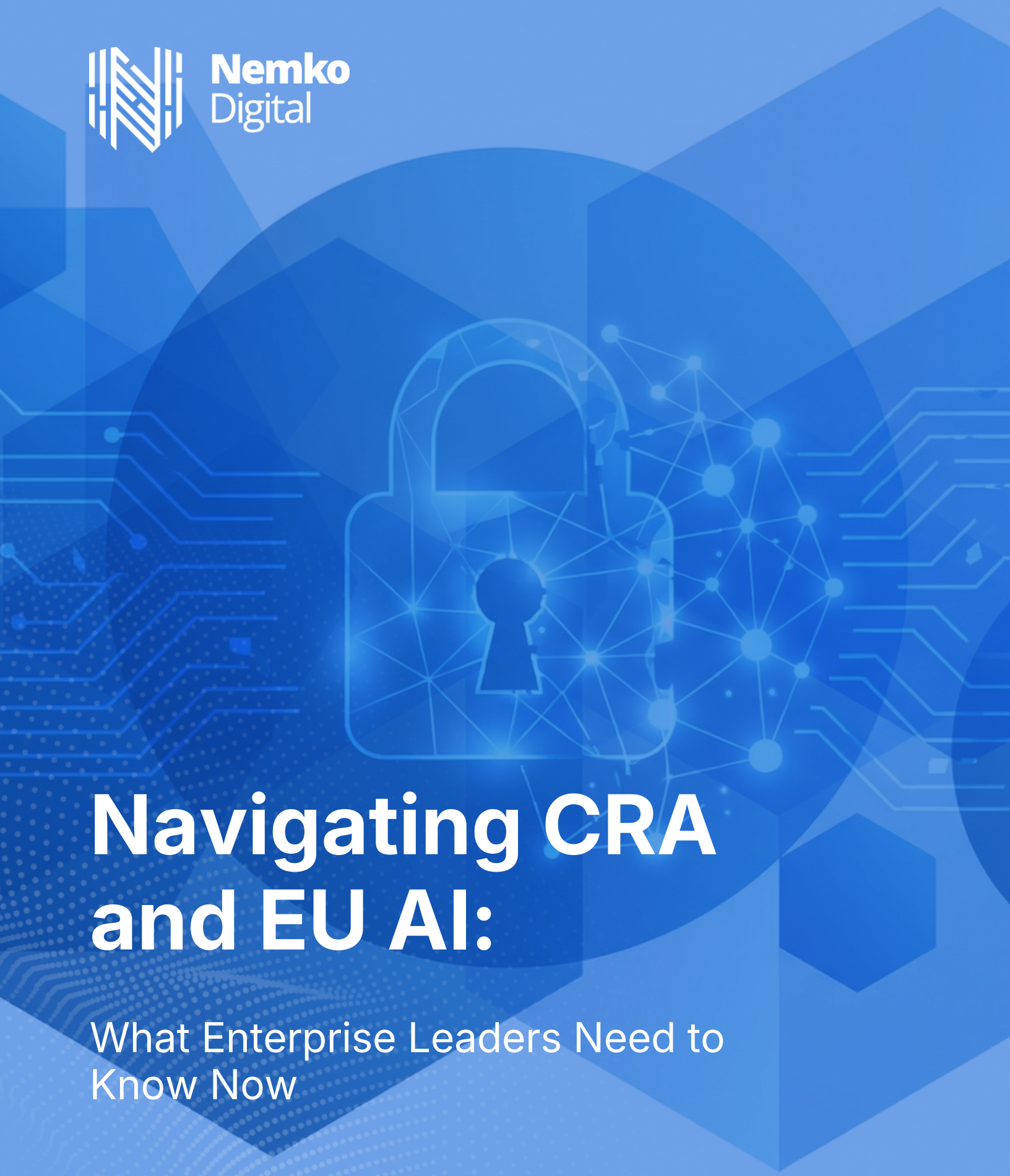
Nemko Digital



Navigating CRA and EU AI:

What Enterprise Leaders Need to Know Now

Break the AI Act and CRA silos. For high-risk AI embedded in digital products, Article 15 and CRA Article 12 intersect: align AI governance with secure-by-design and vulnerability management to cut duplicate controls and streamline compliance.

Navigating CRA and EU AI Act: What Enterprise Leaders Need to Know Now

For many enterprises, EU AI Act and EU Cyber Resilience Act (CRA) compliance is a drag on the business. Controls are duplicated across teams. Evidence is produced twice in different formats. Security, risk, product, and AI departments trip over each other because they are working from different regulatory playbooks.

Yet despite this growing friction, most organizations still manage these two regulations in silos. The CISO owns technical cybersecurity documentation and product security obligations under the CRA, while the CAIO or CRO separately assesses AI risk, governance, and controls under the EU AI Act.

This divide and conquer approach may be a reality today, but it is quickly becoming a liability. AI systems are increasingly embedded in products with digital features, placing them directly at the intersection of both regulations. The same system can be simultaneously high-risk under the EU AI Act and subject to CRA security, vulnerability management, and documentation requirements.

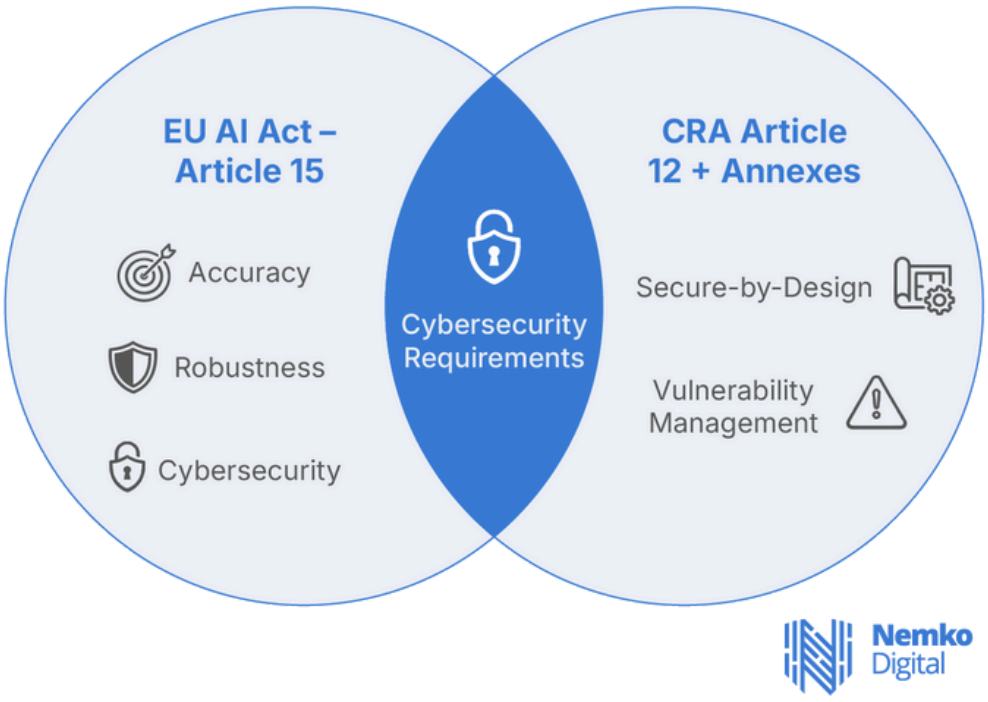
How much inefficiency and risk the business can afford while managing them apart?



EU AI Act Article 15 and CRA Article 12: Where Regulations Meet in the Middle

Both regulations require that AI systems must be robust, secure and cyber resilient across the entire AI/ML lifecycle.

This similarity surfaces as the EU AI Act's Article 15 which states "High-risk AI systems shall be designed and developed in such a way that they achieve an appropriate level of accuracy, robustness, and cybersecurity, and that they perform consistently in those respects throughout their lifecycle" and CRA's Article 12 rule that "Without prejudice to the requirements relating to accuracy and robustness set out in Article 15 of Regulation (EU) 2024/1689, products with digital elements which fall within the scope of this Regulation and which are classified as high-risk AI systems pursuant to Article 6 of that Regulation shall be deemed to comply with the cybersecurity requirements set out in Article 15 of that Regulation."



The intersection of EU AI Act Article 15 and CRA Article 12: Where cybersecurity requirements converge for high-risk AI systems.

Meanwhile, there are two Annexes to CRA's Article 12 that specifically outline how cybersecurity can be achieved.

- **CRA Annex I Part I:** Secure-by-design and secure-by-default architecture, protection against known vulnerabilities, secure configuration, logging, and protection of data and communications.
- **CRA Annex I Part II:** Vulnerability handling, coordinated vulnerability disclosure, security update processes, and lifecycle risk management.

Conformity Presumption Between EU Regulation

If your company launches a high-risk AI system that is also a product with digital elements and it meets Parts I and II of CRA Annex I: Parts I and II, the system is presumed to comply with cybersecurity of Article 15 AI Act (not accuracy or robustness).



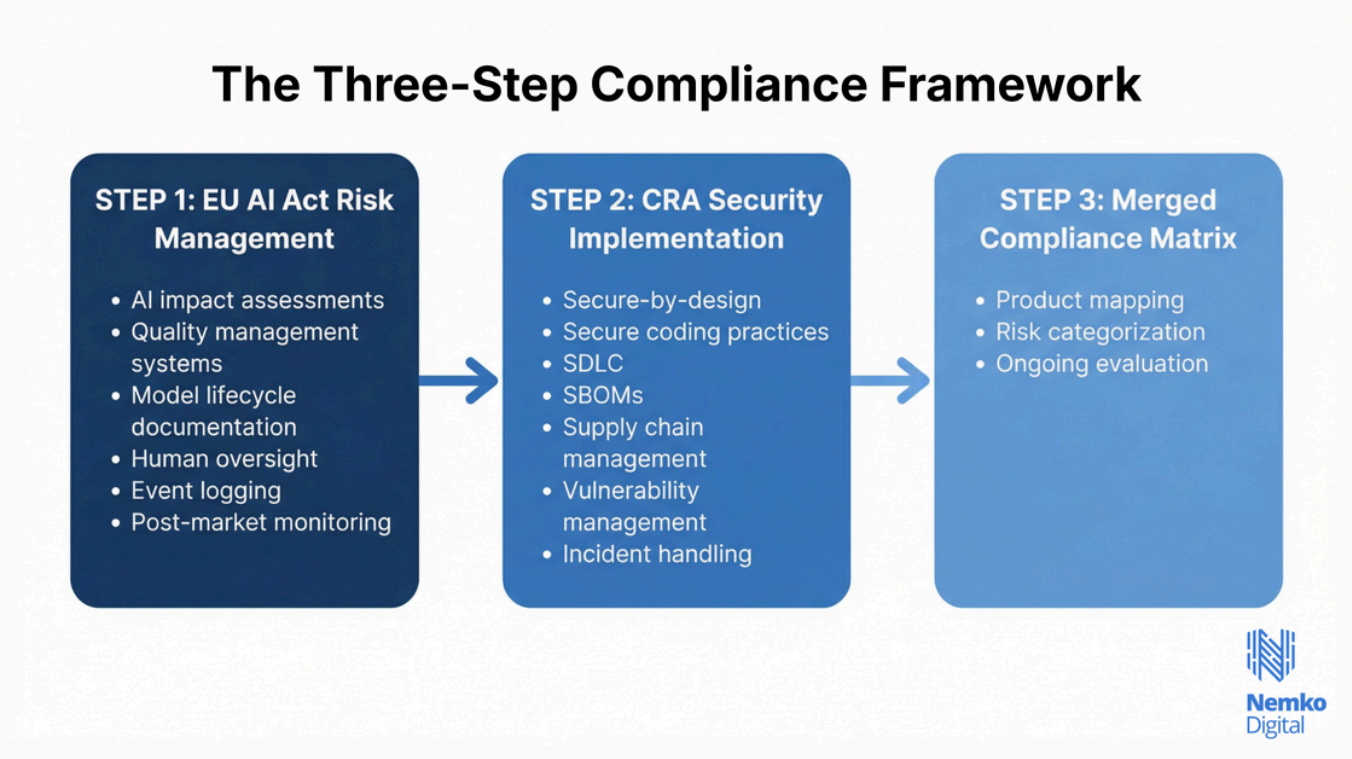
The EU AI Act and the Cyber Resilience Act are not incidental overlaps but complementary. Together, they are designed to empower organizations govern AI systems and digital products through a shared set of risk, security, and lifecycle controls rather than parallel compliance tracks.

When applied in concert, core requirements such as risk assessment, secure-by-design development, incident handling, and documentation can be satisfied once and submitted across both regulations for evidence. The result is fewer redundant controls and a smoother handoff between AI governance and product security teams.

Prioritizing Compliance: Which Comes First? CRA or EU AI Act

First, it's best to evaluate whether your AI systems fall under the EU AI Act's high-risk category, because that classification shapes your overall AI plan, system design and governance approach.

Once you have determined that your system and/or product is classified as AI high risk, start with EU AI Act and then, supplement compliance with CRA requirements. This empowers executives to leverage EU conformity presumption between EU AI Act Article 15 and CRA Article 12 to reduce compliance obligation redundancy.



Strategic compliance roadmap: A 3-step framework for navigating CRA and EU AI Act requirements efficiently.

The Three-Step Compliance Framework

Step 1

Manage and govern AI high risks (AI impact assessments, quality management systems, model lifecycle documentation, human oversight obligations, event logging and post-market monitoring) to uphold EU AI Act requirements.

Step 2

In parallel (or shortly thereafter), ensure your software and/or devices running AI are designed, developed and maintained with strong security before real-world use and post- deployment. This includes secure-by-design development and ongoing vulnerability management for any digital product that delivers or hosts those AI systems.

You can leverage CRA-style security practices (secure coding practices, SDLC, SBOMs, supply chain management governance, incident handling) to serve as evidence for EU AI Act system robustness proof and technical controls. Vice versa, you can use outputs from the EU AI Act risk management operations in Step 1 to inform CRA lifecycle security obligations.

Step 3

Establish a single, cross-functional EU AI Act and CRA compliance program. This step is an intentional executive decision to run AI governance and product security compliance under one integrated program with clear ownership.

Start with a unified inventory of products, software, AI systems, models, and use cases in a single matrix. Classify AI systems by intended purpose and assign EU AI Act risk categories on an ongoing basis while simultaneously flagging CRA applicability for any products with digital elements. This central view reflects where the regulations deliberately intersect.

In practice, an AI system cannot meet EU AI Act governance requirements if the software and hardware it runs on fail the CRA's secure-by-design and vulnerability management mandates. When you manage both under one program, you align controls, reduce duplication, and make integrated AI and product security governance a conscious, auditable C-suite choice.

About the Author



Caryn Lusinchi

As global leader in AI governance and risk management, Caryn helps enterprises navigate the complex intersection of emerging technologies and regulatory frameworks. Drawing on expertise in the EU AI Act, GDPR, EU Data Act, CRA, GPSR, ISO 42001, and NIST AI RMF, she drives executable strategy that balances innovation with responsibility. Additionally is an accredited AI Auditor (FHCA) in EU AI ACT and GDPR and a Non-Resident Senior Fellow in AI and Global Governance in Brussels, Belgium.

Nemko Digital