Deloitte.

Whitepaper: Navigating the EU Cyber Resilience Act

A Strategic Guide to Compliance, Risk Mitigation, and Competitive Advantage

August, 2025

MAKING AN IMPACT THAT MATTERS since 1845

Executive summary

The EU's Cyber Resilience Act (CRA) is a new European regulation that sets mandatory cybersecurity requirements for all products with digital elements sold in the EU. These products include industrial equipment, consumer electronics, software and connected devices. It shifts responsibility for security from end-users to manufacturers, making cybersecurity a precondition for market access.

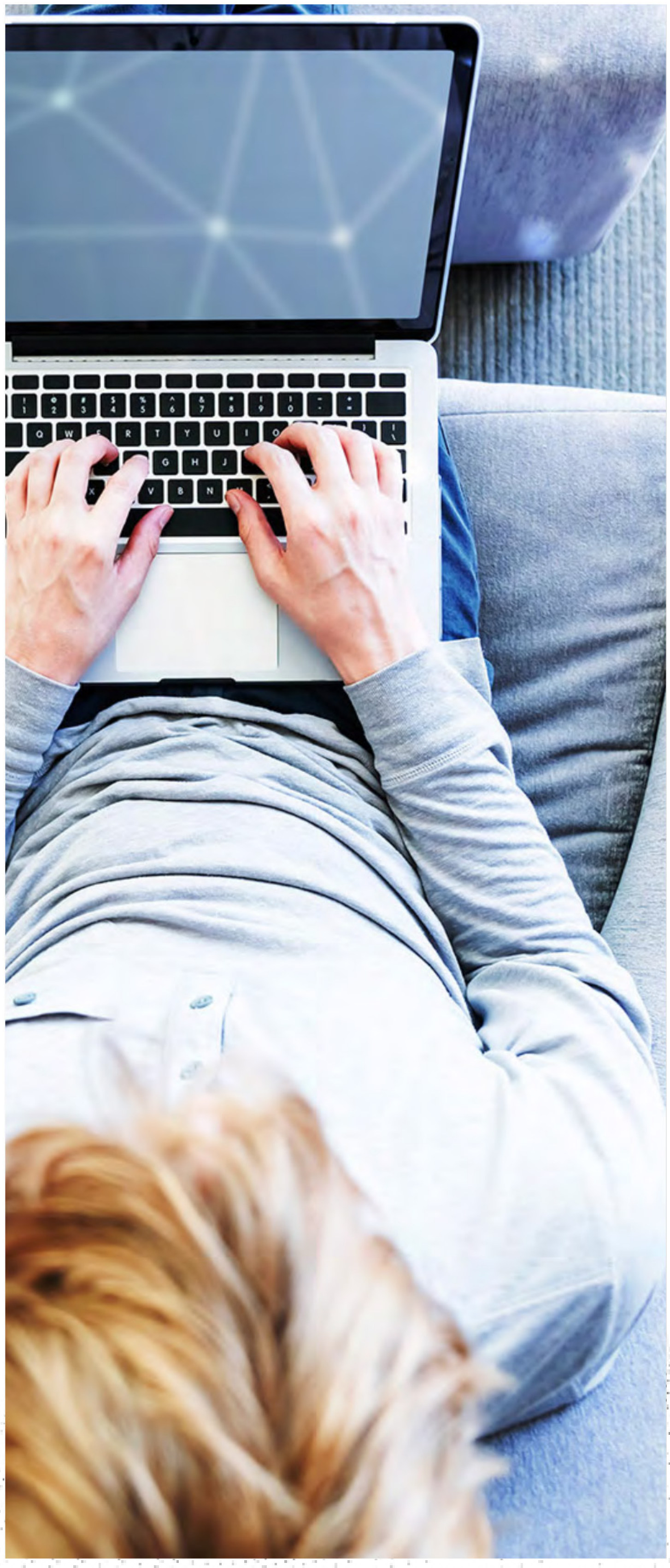
The Cyber Resilience Act is legally in force since 10 December 2024, but its obligations are phased: reporting obligations for actively exploited vulnerabilities and severe incidents begin 11 September 2026. The Act's full application (including CE-marking and conformity-assessment requirements) takes effect 11 December 2027. Regulators have the right to request detailed evidence proving a product's cybersecurity compliance and can order product recalls or impose fines if standards are not met.

Practically the CRA transforms product security from a best practice into an auditable lifecycle requirement:

- manufacturers must be able to issue an early warning within 24 hours of becoming aware of an actively exploited vulnerability,
- provide fuller notifications within the short statutory windows,
- submit reports via the single reporting platform to be operated by ENISA, and
- maintain machine-readable Software Bill of Materials (SBOM) and similar evidences which can be audited by the regulator.

These requirements are not optional engineering add-ons but legally significant controls that force trade-offs across legacy portfolios, third-party dependencies and supplier contracts.

Act now by establishing a dedicated leadership team, completing a thorough product review, and embedding automated security practices and incident readiness into your operations. Organisations that approach CRA readiness as a structured risk management effort will reduce compliance risks and strengthen their position in increasingly security-conscious markets.



Introduction

The Cyber Resilience Act marks a pivotal evolution in the EU's digital single market, addressing the new generation of challenges that have emerged with the increasing use of connected technologies. As digital components become integral to countless products, a harmonized approach to cybersecurity is necessary to ensure a secure, trustworthy, and resilient ecosystem for all. The CRA meets this need by shifting the paradigm of responsibility. It establishes that cybersecurity is not an afterthought or a user's burden, but an essential, non-negotiable component of product design, development, and maintenance, creating a level playing field where security is a precondition for market access.

Are You in Scope?

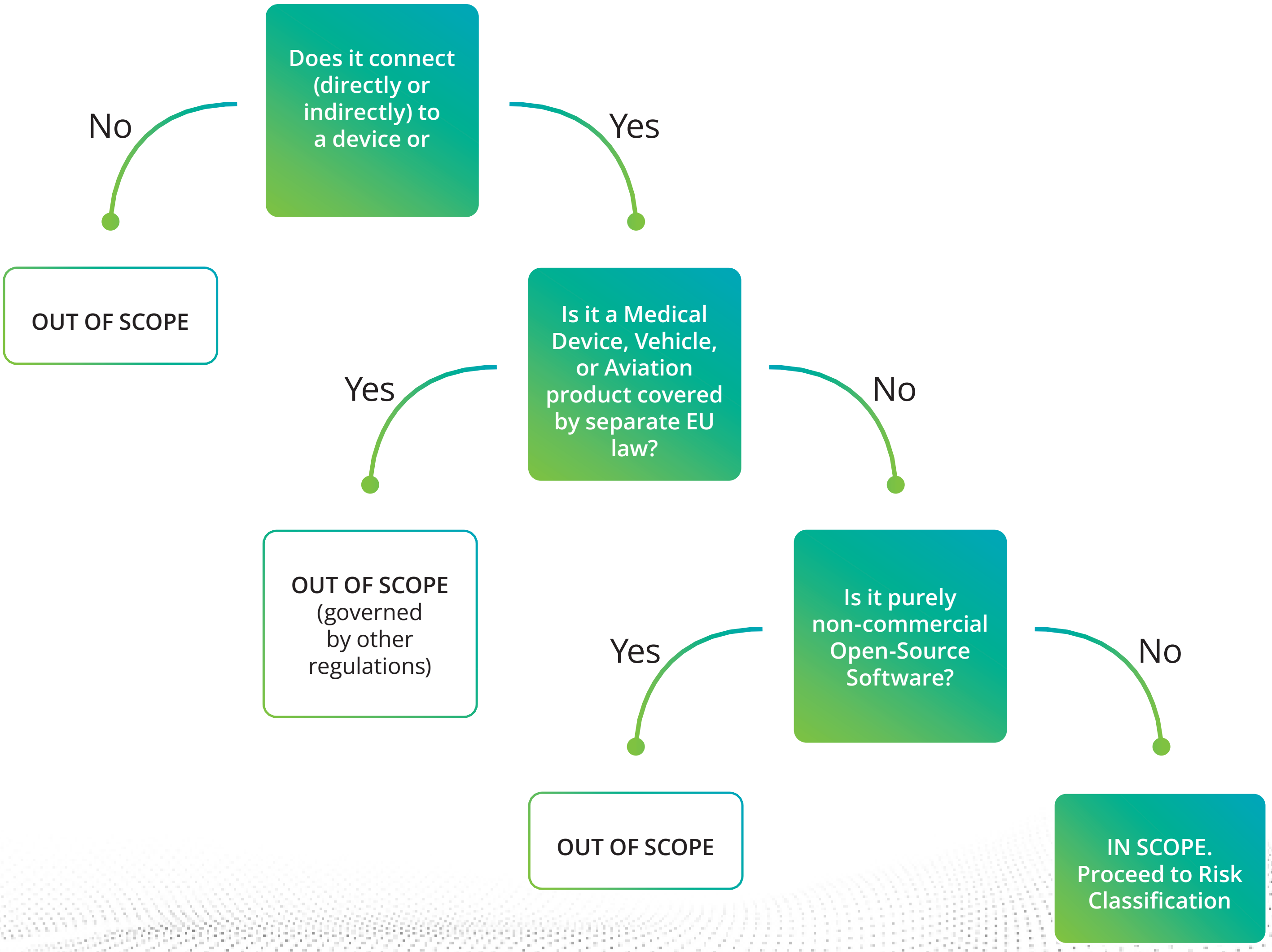
The scope of the Cyber Resilience Act is deliberately broad. Its reach is not confined to tangible hardware but extends deeply into intangible software, including mobile applications, desktop software, and firmware. The guiding principle is straightforward: if your product has a digital component and can connect to a network, it is almost certainly in scope.

CRA Scope Decision Tree

Organisations can use the below decision tree to identify if they are in scope. Special consideration should be given to cloud components of products.

Once in scope, a manufacturer must classify its product's risk level. The vast majority of products will fall into the **Default Category**, permitting a **self-assessment** of conformity. Products with elevated risk are classified as "**Important**" **(Class I)** and require adherence to specific harmonized standards for self-assessment. The most critical products are designated "**Critical**" **(Class II)** and require a **mandatory third-party conformity assessment** by a government-approved "notified body."

Does your product have digital elements?


Does it connect (directly or indirectly) to a device or
No
Yes
OUT OF SCOPE
Is it a Medical Device, Vehicle, or Aviation product covered by separate EU law?
Yes
No
OUT OF SCOPE (governed by other regulations)
Is it purely non-commercial Open-Source Software?
Yes
No
OUT OF SCOPE
IN SCOPE. Proceed to Risk Classification

CRA Compliance Timeline

Roadmap to CRA Compliance
Achieving compliance with the Cyber Resilience Act is an undertaking that requires a structured, multi-year program. This section provides a concrete, three-phase roadmap that organizations can adapt to their specific context, breaking down the journey into manageable, sequential stages.

This initial phase is about establishing control, visibility, and strategic direction.

01. **Establish a CRA Steering Committee:** Assemble a cross-functional team with executive sponsorship, including leaders from legal, compliance, engineering, product management, and supply chain. Assign a clear, single owner (e.g., CISO or Chief Product Officer) responsible for driving the program.

02. **Conduct a Product Portfolio Analysis:** Conduct an exhaustive inventory of every product with a digital element your organisation markets in the EU. Map each item against the CRA's scope and its likely risk classification.

03. **Perform a Gap Analysis:** With a clear picture of what is in scope, assess your current policies, procedures, and development practices against the CRA's requirements to identify and prioritize key deficiencies.

04. **Allocate Budget & Resources:** Secure the necessary funding and personnel to close the identified gaps. This budget must account for new tooling (e.g., SCA for SBOMs, SAST/DAST for testing), extensive training, and potential costs for mandatory third-party conformity assessments for higher-risk products.

This phase is focused on embedding security into the DNA of how your products are designed, built, and tested.

01. **Implement Security by Design & Default:** Mandate threat modeling, adopt and enforce secure coding standards (e.g., OWASP MASVS for mobile), and ensure all products ship with a secure-by-default configuration.

02. **Bolster Supply Chain Security for both software and hardware:** Implement tools and processes to automatically generate a complete and accurate Software Bill of Materials (SBOM) for every product and every update. Next to this, ensure secure sourcing of hardware components and review their security (e.g. encryption). This review of supplier contracts is an undertaking that will require close collaboration between legal, procurement, and engineering, and may necessitate renegotiations.

03. **Establish Robust Security Testing:** Integrate automated security testing tools (SAST/DAST) into your development pipeline and conduct regular, in-depth penetration testing by qualified experts, especially before major product releases.

04. **Prepare Technical Documentation:** Create a standardized template for the "Technical File" that will serve as evidence for CRA compliance for all products.

05. **Formalize Vulnerability Handling:** Publish a clear Coordinated Vulnerability Disclosure (CVD) Policy. Implement a robust internal process to receive, track, assess, and remediate reported vulnerabilities. A mature vulnerability management program is no longer a cost center; it is a direct contributor to brand reputation and customer loyalty.

06. **Plan for Security Updates:** Define and communicate a clear support period for security updates, with a market expectation of at least five years for most products.

This final phase ensures compliance is not a one-time event but a continuous commitment.

01. **Prepare for Incident Reporting:** Develop and test an incident response plan that specifically addresses the 24-hour notification deadline to ENISA for actively exploited vulnerabilities.

CRA challenging areas and ways to tackle them

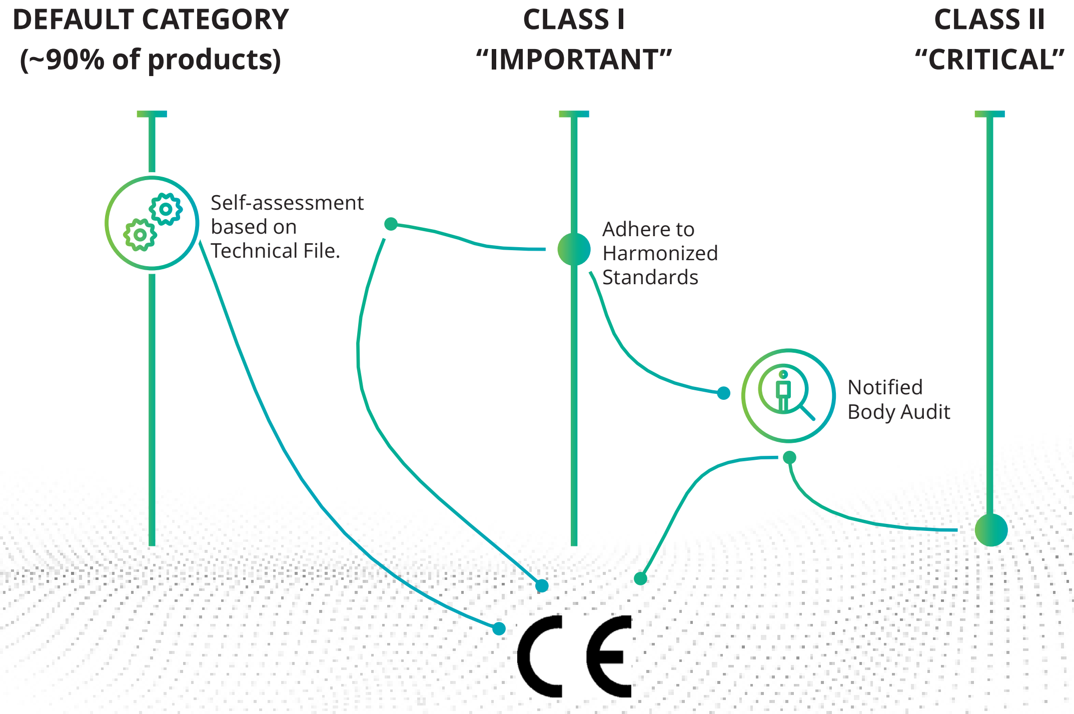
From speaking with clients, the most challenging areas when implementing CRA are:

01. The Software Bill of Materials (SBOM)
The SBOM is a foundational requirement of the CRA. It is a machine-readable inventory of all software components and dependencies in a product. Its purpose is to provide essential transparency for managing vulnerabilities. Beyond compliance, a readily available SBOM is a powerful sales enablement tool for enterprise customers who increasingly mandate supply chain transparency as a condition of purchase. Generating an SBOM requires integrating **Software Composition Analysis (SCA)** tools into the development pipeline. This cannot be a one-time exercise; the SBOM must be regenerated with every new release and forms a core part of the technical documentation.

02. Vulnerability Management and the 24-Hour Reporting
Continuous vulnerability management. Requires a public-facing channel for researchers to report flaws and a internal processes to patch them. The legal deadline to notify ENISA is **within 24 hours** of becoming aware that a vulnerability is being **actively exploited**. This short timeline necessitates a well-rehearsed incident response plan and a designated team ready to act 24/7, requiring input from legal and communications teams.

03. Navigating the Conformity Assessment Paths
Under the CRA, the CE marking evolves to become a visible symbol of cybersecurity assurance. The path to earning this mark depends entirely on your product's risk classification. This is further elaborated on the next page.

CRA Conformity Assessment Paths



Conformity Assessment Paths

The foundation for all paths is the **Technical File**. For **Default Category** products, manufacturers perform a **self-assessment**. For **Class I "Important"** products, manufacturers face a choice between self-assessment (if adhering to standards) or involving a Notified Body. For **Class II "Critical"** products, a mandatory audit and certification from a **Notified Body** is the only path.

The term "self-assessment" in the context of the CRA can be misleading. It does not imply an informal, casual internal review or a simple check-the-box exercise. Rather, it is a formal, structured, and legally binding process where the manufacturer assumes full liability for their product's conformity.

Think of it not as grading your own homework, but as preparing your own corporate tax returns. You do the work yourself, but you must follow precise government rules, maintain immaculate records to support every claim, and sign a legal declaration attesting to its accuracy. If you are audited, the burden of proof is entirely on you.

The self-assessment process is anchored by the **Technical File**. This is not a summary document; it is the comprehensive body of evidence that substantiates the claim of compliance. For a self-assessment to be valid, this file must be compiled and maintained. It must contain the proof that the manufacturer has performed its due diligence for every applicable requirement of the Act.

A robust and defensible self-assessment procedure involves several concrete steps:

01. Compilation of Evidence: The first step is the methodical creation of the Technical File, gathering all required artifacts, test results, and design specifications.

02. Internal Verification and Validation: Before any declaration is made, the completed Technical File and the product itself should undergo an internal review by a function separate from the development team, such as a Quality Assurance or internal audit team.

03. The EU Declaration of Conformity: Once internal verification is complete, the manufacturer must draft and sign the official EU Declaration of Conformity. A designated officer of the company formally attests that the specified product conforms to the Cyber Resilience Act.

04. Affixing the CE Mark: Only after the Declaration of Conformity has been signed can the manufacturer legally put the CE marking on the product.

When the CE mark is present, National **Market Surveillance Authorities** across the EU are empowered to select products from the market and demand to see the Technical File at any time. If an authority challenges the product's security, or if a security incident occurs, the burden of proof falls on the manufacturer. Failure to produce a credible and comprehensive file can result in fines, forced product recalls, and significant reputational damage.

Link with other cyber security European legislation

Companies that are in scope of NIS2 or DORA might also be in scope of the CRA. At the moment no concepts like lex specialis between DORA and NIS2, are defined in the CRA. However the European Commission might adopt delegated acts that specify exceptions.

Medical devices fall under different regulations like the MDR and IVDR. The MDR (Regulation (EU) 2017/745), which came fully into force in May 2021, imposes significantly stricter requirements on the safety and performance of medical devices compared to the previous directives. For in-vitro diagnostics, such as blood glucose testers and pregnancy tests, the IVDR (Regulation (EU) 2017/746) applies.

Companies will need to evaluate for every product individually under which legislations it might fall.

Next steps

The Cyber Resilience Act mandates an operational shift. Requirements for SBOMs, vulnerability management, and formal conformity assessments are extensive and require significant efforts to implement. Organizations should assess how they want to pursue compliance and based on the strategic compliance timeline define concrete steps forward.

Contact

Evert Koks

Director

Cyber Strategy & Transformation

email: **ekoks@deloitte.com**

mobile: **+32 476 65 99 27**

Jens Baetens

Manager

Cyber Defense & Resilience

email: **jbaetens@deloitte.com**

mobile: **+32 495 47 07 16**

Julie Colle

Senior Consultant

Cyber Strategy & Transformation

email: **jcolle@deloitte.com**

mobile: **+32 478 60 84 96**

Deloitte.

About Deloitte
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms.

Deloitte provides audit, tax and legal, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte has in the region of 312,000 professionals, all committed to becoming the standard of excellence.

This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte Network") is, by means of this publication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this publication.