



Cyber Resilience Act (CRA)

KPMG Netherlands

September 2026

KPMG. Make the Difference.



The Cyber Resilience Act (CRA) represents a fundamental shift in how product cybersecurity is regulated across the European Union. It establishes the EU's first horizontal regulatory framework imposing mandatory cybersecurity requirements on a broad range of hardware and software products made available on the EU market.

Manufacturers and other economic operators must demonstrate that applicable cybersecurity requirements have been addressed before covered products can be placed on the market and carry the CE marking.

This shift reflects the reality that products are increasingly software-based, connected and dependent on complex digital supply chains. As a result, product security is becoming a strategic business responsibility, not merely an IT or engineering matter. Organisations must be able to demonstrate that cybersecurity is embedded from design and development through to placing the product on the market, operation, maintenance, vulnerability handling and the provision of security updates during the applicable support period.

The challenge for many organisations is that CRA defines the cybersecurity outcomes that must be achieved, while leaving manufacturers responsible for selecting and implementing appropriate technical and organisational measures. As a result, organisations must translate concepts such as secure-by-design and secure-by-default development, cybersecurity risk assessment, vulnerability handling and lifecycle security into practical governance, development and operational processes.

This is where emerging standards and existing product-security practices become important. The EN 40000 standards series is being developed to support implementation of the CRA by translating its essential cybersecurity requirements into more detailed technical specifications and assessment criteria. Although key parts remain in draft, they already provide useful direction for product-security processes, documentation and evidence. The following pages combine this regulatory overview with practical implementation insights.

For many organisations, the first step is still to recognise that the CRA affects them. Those that do recognise this are asking a key question:

How can we ensure and demonstrate that cybersecurity is embedded in our products and throughout the product lifecycle?"

Background and relevance

The increasing digitalisation of products has fundamentally changed the cybersecurity landscape. Products that were once largely mechanical now contain software, connectivity and complex digital dependencies, including embedded software, cloud services and third-party components. As a result, cyber risks increasingly extend beyond internal systems and directly affect the products organisations place on the market. A security vulnerability in a connected product can impact customers, operators and manufacturers alike.

CRA is the European Union’s response to this changing risk landscape and becomes applicable in phases. Vulnerability-reporting obligations apply from 11 September 2026, including to products already on the market. From 11 December 2027, the full CRA requirements apply to products placed on the market from that date.

At the same time, products are expected to remain secure throughout their lifecycle. This requires manufacturers to not only design and develop products securely, but also manage vulnerabilities, provide security updates free of charge and maintain supporting documentation during the applicable support period.

Product security has therefore become a business responsibility that spans engineering, operations, legal, compliance, sales and risk management functions. Under CRA, the support period must reflect the time the product is expected to be in use and must generally be at least five years, unless the product is expected to be used for a shorter period.

The challenge is how to embed these requirements throughout the product lifecycle and demonstrate

Scope and applicability

CRA affects a wide range of organisations that develop, manufacture, import or distribute **Products with Digital Elements (PDEs)** on the European market. A useful rule of thumb is: if a hardware or software product includes a direct or indirect data connection to another device or network, it is likely relevant for the CRA. Think of smart home devices, connected machinery, embedded software, operating systems and software applications. Close to home examples are connected central heating, thermostats, refrigerators, sound systems, connected barbecues, televisions, smart meters, air conditionings, but also cars, connected lamp bulbs, alarm systems etc. etc. Standalone SaaS is generally excluded. While the CRA is often associated with **manufacturers**, it also places obligations on **importers** and **distributors**.

Who is this for?



Manufacturers placing connected products on the EU market.



Producers of IoT, OT, industrial and smart-device products.



Vendors of embedded software, firmware, operating systems, routers and digital components.



Product teams responding to supply-chain security expectations, market access requirements and lifecycle security.



Importers and distributors responsible for verifying product compliance before making products available on the EU market.

For many organisations, the challenge is not simply determining whether they develop software but identifying where digital functionality exists across their products and supply chains, which legal entity acts as the manufacturer or other economic operator, and whether any exclusions apply.

CRA timeline: where are we now?

The Cyber Resilience Act has already entered into force (December 2024), but its obligations become applicable in phases (see Timeline below). This gives organisations a limited window to assess scope, establish governance, adapt development processes and prepare the documentation and evidence required to demonstrate compliance.

A key consideration for manufacturers is that **vulnerability-reporting obligations are applicable from 11 September 2026**, more than a year before the full regulation takes effect. Organisations should therefore ensure that vulnerability-handling and reporting processes are established well in advance of the final compliance deadline.

Regulatory timeline



What does CRA require?

The Cyber Resilience Act introduces a seemingly simple principle: products should be secure by design, remain secure throughout their lifetime, and manufacturers, distributors, and importers should be able to respond quickly when vulnerabilities emerge.

1. Integrate security throughout product development

Cybersecurity should be embedded into the design and development process from the outset, rather than being addressed after a product has been developed or released.

2. Establish effective vulnerability management

Organisations should maintain processes to identify, assess, remediate and monitor vulnerabilities affecting their products, including vulnerabilities in third-party software and open-source components. Maintaining visibility of product components, for example through Software Bills of Materials (SBOMs), can support vulnerability management and impact assessment.

3. Maintain security throughout the product lifecycle

Security responsibilities extend beyond product launch. Manufacturers are expected to monitor emerging risks and provide security updates and remediation measures where appropriate.

4. Maintain evidence of compliance

Organisations should retain appropriate documentation and technical evidence demonstrating how cybersecurity requirements have been addressed and managed over time. This may include documentation relating to product architecture, dependencies and Software Bills of Materials (SBOMs).

5. Demonstrate compliance before market placement

Before placing products on the EU market, manufacturers must demonstrate compliance with applicable CRA requirements and complete the relevant conformity assessment activities.

6. Establish incident reporting and response capabilities

Organisations must be able to identify, assess and escalate vulnerabilities and cybersecurity incidents in a timely manner. From 11 September 2026, actively exploited vulnerabilities and severe incidents, including in legacy products, are subject to mandatory reporting within prescribed timelines.

CRA and the wider regulatory landscape

The Cyber Resilience Act does not exist in isolation. It forms part of a broader European regulatory landscape requiring organisations to demonstrate both operational cyber resilience and product security. Understanding how the CRA interacts with other regulations can help organisations align governance, processes and controls while addressing each regulation’s distinct requirements.

CRA and the Network and Information Systems Directive 2 (NIS2)

CRA and NIS2 address different aspects of cybersecurity. In practical terms, NIS2 focuses on the cybersecurity of the organisation and its network and information systems, while CRA focuses on the cybersecurity of products with digital elements. NIS2 addresses operational resilience through cybersecurity governance, risk management and incident reporting, while CRA establishes product cybersecurity requirements and associated vulnerability-handling processes. Compliance with one does not automatically demonstrate compliance with the other.

For organisations that develop or manufacture connected products, both regulations could apply and may rely on shared capabilities, including governance, cyber risk management, vulnerability management and incident response. Organisations should therefore align relevant ownership, processes and controls across both programmes while maintaining clear evidence for their separate legal obligations.

CRA and the Radio Equipment Directive (RED)

Many organisations have already prepared for the cybersecurity requirements under the Radio Equipment Directive (RED). While the RED framework itself has been in force since 2016, certain cybersecurity requirements only became applicable on 1 August 2025. The RED cybersecurity requirements applies to specified categories of radio equipment, while the CRA scope is wider and has significantly broader requirements.

Good to know: The RED will continue to exist after 2027, but its cybersecurity provisions are expected to be replaced by the CRA for products that fall within CRA scope. The RED will still apply for its traditional topics such as radio spectrum use, electromagnetic compatibility (EMC), and health and safety requirement.

From December 2027, you will likely still need to comply with RED requirements for radio-related aspects of your product, but cybersecurity compliance will primarily be assessed against the CRA.





What CRA implementation is teaching us

Although the intent of the CRA is straightforward, implementation is often challenging because regulatory requirements must be translated into practical product, governance and lifecycle processes. While many of these observations arise from implementation work with manufacturers, several themes are equally relevant for importers and distributors. In our experience, organisations repeatedly encounter the following lessons:

Understanding what is actually in scope

Many organisations struggle to determine which products, product variants, software components and third-party dependencies fall within scope. In practice, CRA scoping is rarely just a product inventory exercise. Organisations that make progress early establish a defensible scope position covering product families, embedded software, cloud-supported functionality and supply-chain dependencies.

Governance is often one of the biggest gaps

Many organisations initially focus on technical controls. Unlike IT security, product security often lacks central governance and clear ownership. Effective CRA implementation requires ownership, accountability, escalation and collaboration across the product lifecycle. Leading organisations assign clear responsibility for product cyber risk, vulnerability handling and reporting decisions.

Product security is a different discipline from enterprise security

Many organisations have mature IT security capabilities, while OT security capabilities are continuing to develop. However, securing products throughout their support period requires dedicated capabilities for vulnerability handling, security updates, PSIRT processes and regulatory reporting. This is driving dedicated product-security operating models spanning Product, Engineering, Security, Legal and Compliance functions.

CRA introduces lifecycle accountability

Secure-by-design development remains essential, but it is only one part of CRA readiness. Legacy products may require reporting, but not free updates. Organisations must also maintain evidence, manage vulnerabilities, provide security updates, assess reportable events and support products throughout the applicable support period. The most successful implementations treat product security as a lifecycle responsibility rather than a development activity that ends at product launch.

Vulnerability reporting readiness is often underestimated

For many organisations, the challenge is not identifying vulnerabilities or incidents, but coordinating assessment, escalation, decision-making and reporting across multiple teams within the required timelines. In practice, delays frequently arise during handovers between teams rather than during the technical analysis itself. Reporting readiness is therefore driving investment in governance, PSIRT capabilities and cross-functional exercises.

Third-party dependencies require greater visibility

Manufacturers remain responsible for cybersecurity risks introduced through integrated third-party components. Visibility into suppliers, software components and support arrangements is therefore becoming a key prerequisite for vulnerability management, impact assessment and CRA compliance. Increasingly, organisations are linking supplier oversight, SBOM management and vulnerability processes rather than treating them as separate activities.

Key takeaway

The organisations making the most progress treat CRA readiness as a product-security transformation that combines scope, governance, secure development, vulnerability management, supplier oversight and lifecycle support, rather than as a standalone compliance project.

What organisations should do now

- 1. Determine scope** – Identify products with digital elements and assess CRA applicability across business units, product portfolios and third-party dependencies.
- 2. Classify requirements** – Determine applicable CRA obligations, conformity routes and relevant product-security standards.
- 3. Assess current capabilities** – Evaluate existing product-security practices and identify gaps in governance, secure development, vulnerability management and documentation.
- 4. Establish product-security governance** – Define ownership, accountability and decision-making responsibilities, aligned with broader cybersecurity, risk and compliance programmes.
- 5. Establish vulnerability handling and reporting capabilities** – Strengthen PSIRT, vulnerability disclosure and vulnerability management processes. Ensure actively exploited vulnerabilities and severe incidents can be assessed, escalated and reported within regulatory timelines.

Prepare for full CRA compliance

- 1. Embed secure product development** – Strengthen secure-by-design and secure development lifecycle practices across development and maintenance activities.
- 2. Expand in-market product-security operations** – Mature product monitoring, remediation, patch management and lifecycle support processes.
- 3. Prepare compliance evidence and documentation** – Build the technical documentation, security records, traceability and evidence required for conformity assessment and CE-marking activities.

How KPMG can help

- KPMG combines global delivery capacity with specialist legal, CRA, OT, IEC 62443, EN 40000 and product-security expertise. Rather than addressing regulations in silos, we help organisations address CRA alongside related cybersecurity, product-safety and resilience requirements through one integrated approach.**
- ✓ **Assessment, scoping and regulatory insights** – Determine whether the CRA applies, identify affected products, assess current product-security capabilities, and identify gaps against CRA and IEC 62443 requirements.
 - ✓ **Integrated product-security capability** – Embed security into product development, establish product-security governance and implement the vulnerability management and lifecycle-security processes required for CRA compliance and broader product-security objectives.
 - ✓ **Product security operations and implementation support** – Design and implement PSIRT, vulnerability management, reporting and governance processes, supported by practical workshops, templates and action plans.
 - ✓ **Compliance readiness and conformity assessment support** – Prepare the documentation, evidence and traceability needed to demonstrate compliance and support conformity assessment and CE-marking activities.
 - ✓ **ServiceNow implementation and enablement** – Implement workflows and supporting processes in ServiceNow for vulnerability management, PSIRT operations, evidence management, monitoring and reporting.



Ronald Heil
Partner - Cyber & TechLaw
KPMG Advisory N.V.

heil.ronald@kpmg.nl
+31 6 51369785



Mart Meijerink
Manager - Cyber & TechLaw
KPMG Advisory N.V.

meijerink.mart@kpmg.nl
+31 6 83300812



Luc Jansen
Sr. Consultant - Cyber & TechLaw
KPMG Advisory N.V.

jansen.luc@kpmg.nl
+31 6 53547269

Our experts