BCLP. Client Intelligent

Insights

THE CYBER RESILIENCE ACT IS REWRITING THE RULES OF DIGITAL PRODUCTS SAFETY

Nov 07, 2025

The EU Cyber Resilience Act (Regulation (EU) 2024/2847) ("CRA") establishes mandatory cybersecurity requirements for products with digital elements, encompassing both hardware and software products that connect to networks or process data, with the intent of providing a more secure, transparent and responsive product ecosystem in the European market.

Central to the CRA is the establishment of a cascading chain of responsibility throughout the product lifecycle, whereby manufacturers bear primary obligations, whilst importers and distributors assume secondary duties including verification of compliance and reporting of non-conformities to competent authorities. Manufacturers must integrate cybersecurity from the design phase onwards, ensuring continued security throughout production, market placement, and post-market phases.

These requirements have raised significant concerns among economic operators of various size regarding implementation complexity and resource demands. Nevertheless, manufacturers must fundamentally rethink their development, production, and post-market processes to ensure compliance with the CRA for all future products placed on the European market.

WHICH ENTITIES ARE WITHIN SCOPE?

The Cyber Resilience Act applies to economic operators involved in the design, development, manufacturing, and distribution of products with digital elements. Its scope includes:

1. **Manufacturers**: European or foreign entities that develop or manufacture products with digital elements, or have such products designed, developed, or manufactured, and market them under their own name or trademark. This encompasses manufacturers of:
    - Hardware products with digital elements (e.g., IoT devices, routers, smart appliances, connected industrial equipment)
    - Software products, including standalone software and firmware

- Remote data processing solutions (e.g., cloud-based applications, web services, mobile applications)

2. **Importers**: Entities established within the EU, placing products with digital elements from third countries onto the EU market.
3. **Distributors**: Entities in the supply chain, other than manufacturers or importers, that make products with digital elements available on the market.
4. **Providers of Remote Data Processing Solutions**: Entities offering software products that enable data processing at a distance, including:
   - Software-as-a-Service (SaaS) platforms,
   - Cloud-based applications and services,
   - Web-based software solutions,
   - Mobile applications with backend processing.

The CRA does not apply to products already covered by sector-specific EU cybersecurity legislation, including:

- Medical devices (covered by Regulations 2017/745 and 2017/746);
- Aviation equipment (covered by Regulation 2018/1139);
- Motor vehicles (covered by Regulations 2018/858 and 2019/2144);
- Maritime equipment (covered by Directive 2014/90/EU).

Additionally, the CRA excludes:

- Spare parts made available on the market to replace identical components in products with digital elements manufactured according to the same specifications as the components that they are intended to replace,
- Products developed or modified exclusively for national security or military purposes,
- Free and open source software developed or supplied outside the course of commercial activity.

The CRA applies irrespective of where the manufacturer or other economic operator is established, provided that the products with digital elements are placed on the EU market or put into service within the EU. This extraterritorial application ensures that all products available to EU consumers and businesses meet the regulation's cybersecurity standards, regardless of their origin.

WHAT ARE THE KEY OBLIGATIONS OF PRODUCT MANUFACTURERS?

Under the CRA, manufacturers bear primary responsibility for ensuring products with digital elements meet essential cybersecurity requirements throughout their lifecycle. From 11 December 2027, these obligations include:

SECURITY BY DESIGN AND BY DEFAULT

(Article 13): Manufacturers must ensure that products with digital elements are designed, developed, and produced in accordance with essential cybersecurity requirements set out in Annex I. This includes implementing appropriate technical and organizational measures to manage cybersecurity risks, ensuring products are delivered without known exploitable vulnerabilities, and configuring products securely by default (e.g., unique passwords, minimal attack surface, secure default settings).

RISK ASSESSMENT AND TECHNICAL DOCUMENTATION

(Articles 13 and 31): Manufacturers must conduct comprehensive cybersecurity risk assessments identifying potential risks throughout the product's lifecycle and implement appropriate mitigation measures. They must compile technical documentation demonstrating conformity with essential requirements, including risk assessments, security architecture descriptions, and evidence of compliance with harmonised standards where applicable.

CONFORMITY ASSESSMENT PROCEDURES

(Articles 13 and 32, Annex VIII): Depending on product classification, manufacturers must undergo appropriate conformity assessment procedures to guarantee compliance with cybersecurity requirements:

- A self-assessment procedure :
  - For standard products and class I important products.
  - The manufacturer declares conformity on sole responsibility.
  - The manufacturer shall take all measures necessary so that the design, development, production and vulnerability handling processes and their monitoring ensure compliance with the essential cybersecurity requirements of the products with digital elements and its processes.

- An EU-type examination covering design and development followed by a self-assessed production phase:
  - For standard products, class I & class II important products, and critical products (unless certification through a European certification scheme is required as a mandatory provision by the Commission).
  - A two-stage process combining design assessment (the technical design and development of a product with digital elements and the vulnerability handling processes put in place by the manufacturer) with production control (the manufacturer fulfils specific obligations and ensures and declares that the products with digital elements concerned are in conformity with the type described in the EU-type examination certificate).
  - Carried-out by a notified body.
- Quality insurance.
  - For standard products, class I & class II important products, and critical products (unless certification through a European certification scheme is required as a mandatory provision by the Commission).
  - A Comprehensive quality management system approach covering the entire product lifecycle.
  - Carried-out by a notified body.
- European cybersecurity certification scheme (EUCC):
  - For all product categories (standard, class I & II important, and critical products). currently voluntary unless the Commission mandates certification for specific critical product categories through delegated acts.
  - Based on the internationally recognized Common Criteria (ISO/IEC 15408), applicable to ICT products.
  - Certificates valid for maximum five years with possible extension; timelines vary by assurance level (several months for substantial, longer for high) and depend on conformity assessment body capacity and product complexity.

PRESUMPTION OF CONFORMITY

Article 27 of the CRA establishes a presumption of conformity whereby products complying with harmonized standards, common specifications, or European cybersecurity certification schemes are legally presumed to meet the CRA's essential cybersecurity requirements without further demonstration. This provides regulatory relief for manufacturers, simplifies conformity

assessment procedures, and ensures legal certainty and market access. Harmonized standards are currently being developed under Commission Mandate M/606, with delivery expected by 30 November 2027.

SECURITY SUPPORT AND UPDATES

(Article 13): Manufacturers must provide security updates for products for at least five years from the date of placing on the market, or throughout the expected product lifetime if shorter. These updates must address identified vulnerabilities and be provided free of charge. Manufacturers must clearly communicate the security support period to users before purchase.

USER INFORMATION

(Article 13): Manufacturers must provide clear, comprehensive instructions and security-related information to users, including:

- Contact details for reporting vulnerabilities,
- The support period,
- Instructions for secure installation, deployment, and configuration,
- Information about known vulnerabilities and available updates,
- Guidance on secure use and decommissioning.

CE MARKING AND DECLARATION OF CONFORMITY

(Articles 28 to 30, Annexes V and VI): Manufacturers must affix CE marking to compliant products before placing them on the market, signifying conformity with all applicable requirements. They must draw up an EU declaration of conformity identifying the product and declaring that it meets the CRA's essential requirements, and make this declaration available to market surveillance authorities for ten years.

VULNERABILITY MANAGEMENT AND INCIDENT REPORTING

(Article 14): Manufacturers must establish and maintain processes to identify, handle and report vulnerabilities and incident.

RECORD-KEEPING

(Article 13): Manufacturers must maintain records of non-conformities, vulnerabilities, and incidents for ten years after the product has been placed on the market, making these available to market surveillance authorities upon request.

DUTY TO TAKE CORRECTIVE ACTION

(Article 54): Where manufacturers have reason to believe that products they have placed on the market are not in conformity with the CRA, they must immediately take corrective measures to bring the product into conformity, withdraw it, or recall it. They must inform distributors, importers, and market surveillance authorities of the non-conformity and corrective actions taken.

OTHER ECONOMIC OPERATORS' OBLIGATIONS

(Articles 19 & 20): Unlike manufacturers, importers and distributors share similar obligations focused on verification and market surveillance, though importers bear more extensive responsibilities. Both must verify compliance before placing or making products available on the market, act on non-compliance by refusing market access, cooperate with authorities by providing documentation upon request, and report vulnerabilities to the manufacturer. Each have additional obligations, but the obligations of both are contingent on the manufacturer's compliance

As an EU regulation, the CRA is directly applicable across Member States, with enforcement delegated to national market surveillance authorities. Each Member State must establish effective, proportionate, and dissuasive penalties for infringements, with maximum fines reaching up to €15 million or 2.5% of the undertaking's total worldwide annual turnover for the preceding financial year, whichever is higher. Non-compliance may result in product withdrawal orders, prohibition of market placement, financial penalties, and reputational damage, particularly where vulnerabilities lead to security incidents affecting users or critical infrastructure.

PREPARING FOR EARLY REPORTING OBLIGATIONS UNDER ARTICLE 14

Under Article 14 of the CRA, manufacturers are subject to vulnerability and incident reporting obligations that become applicable significantly earlier than the regulation's general requirements.

Whilst the CRA's substantive provisions take effect from 11 December 2027, Article 14's reporting obligations apply from 11 September 2026, over a year earlier, requiring manufacturers to establish

compliant processes well in advance. Reporting obligations will apply to any and all digital products falling into the scope of the CRA regardless of the time they are placed on the EU market.

Article 14 establishes a three-stage reporting framework designed to enable ENISA and national CSIRTs (Computer Security Incident Response Teams) to monitor emerging cybersecurity threats and coordinate rapid responses to actively exploited vulnerabilities and severe incidents. The framework imposes strict timelines that manufacturers must observe:

- **24-hour early warning**: Notification to ENISA and national CSIRTs via the single report platform, and users upon becoming aware of actively exploited vulnerabilities or severe incidents,
- **72-hour detailed report**: Technical description, affected products, severity assessment, and mitigation measures,
- **14-day final report for vulnerabilities or 1 month for incidents**: Root cause analysis, corrective actions, and preventive measures following remediation,
- Continuous monitoring: Ongoing vulnerability detection including third-party components and supply chain risks.

To ensure compliance before September 2026, manufacturers should establish vulnerability management infrastructure, including monitoring systems, incident response procedures, technical integration with ENISA reporting platform, and contractual arrangements with suppliers requiring prompt vulnerability disclosure. These processes are essential not only for regulatory compliance but also for demonstrating due diligence in the event of security incidents affecting users or critical infrastructure.

WHAT IS THE COMPLIANCE TIMELINE?

The regulation entered into force on 10 December 2024, but its substantive provisions become applicable progressively to allow manufacturers and economic operators sufficient time to adapt their processes and products.

The CRA establishes the following compliance timeline:

- **11 September 2026**: Article 14 (vulnerability and incident reporting obligations) becomes applicable to manufacturers of products with digital elements already placed on the market, requiring immediate operational readiness for the three-stage reporting framework.
- **11 December 2027**: The CRA's general provisions become fully applicable.

Products lawfully placed on the market before 11 December 2027 are not retroactively subject to CRA obligations. However, if such products undergo a substantial modification after that date, they

must comply with the CRA, and the person making the modification assumes the role of manufacturer for the modified product. A change is considered substantial if it:

- Alters the product's intended purpose,
- Affects its compliance with CRA requirements, or
- Impacts its cybersecurity posture.

The European Commission adopts delegated acts to specify which sub-categories of products are classified as important or critical. When such an act is adopted, the Commission sets the date from which stricter conformity assessment requirements apply, creating a transitional period:

Category of Products	**Transitional Period**
Standard	None
Important	Minimum 12 months before stricter conformity assessment procedures apply, or less than 12 months if justified on imperative grounds of urgency
Critical	Minimum 6 months before mandatory EU certification applies, or less than 6 months if justified for imperative reasons of urgency

During the transitional period, manufacturers may continue placing products on the market under existing assessment rules. After the transitional date, newly placed products must comply with the new important or critical requirements, including notified-body assessment or mandatory EU certification as specified

WHAT STEPS SHOULD YOU TAKE NOW?

With the CRA's reporting obligations taking effect from 11 September 2026 and full applicability from 11 December 2027, manufacturers of products with digital elements must act swiftly to align their operations, technical infrastructure, and contractual arrangements. The following steps are essential to ensure compliance and mitigate legal and commercial risks:

PRODUCT ASSESSMENT AND CLASSIFICATION:

- Conduct a comprehensive inventory of all products with digital elements (hardware, software, and remote data processing solutions) to determine which fall within the CRA's scope.
- Assess product classification (standard, important Class I, Class II or critical) to identify applicable conformity assessment procedures.

CONFORMITY ASSESSMENT PREPARATION:

- Choose the appropriate conformity assessment procedures.
- Prepare the documentation (technical documentation, quality system documentation, etc.)
- Identify and engage notified bodies for EU-type examination or quality system assessment.

DOCUMENTATION:

- Establish internal policies for cybersecurity risk assessment, vulnerability management, and incident response.
- Draft and maintain technical documentation demonstrating conformity with essential requirements for ten years.
- Draw up EU declaration of conformity.

SECURITY SUPPORT:

- Define security support periods (minimum 5 years or expected product lifetime) for all products.
- Pick a single point of contact for user communication on security advisories, vulnerability notifications, and update delivery.

VULNERABILITY MANAGEMENT:

- Establish continuous monitoring systems to identify vulnerabilities in products, including third-party and open-source components.
- Implement processes for managing vulnerability reports from security researchers, users, and suppliers.
- Develop incident response procedures with clear escalation paths to meet the three-stage reporting requirements.

CONTRACT REVIEW AND REDRAFTING:

- Review supplier agreements to include obligations for prompt vulnerability disclosure, timelines aligned with Article 14, and clarity on reporting responsibilities for third-party components.
- Update customer agreements to address security support periods, update delivery mechanisms, vulnerability reporting procedures, and liability limitations.
- Revise distributor and importer agreements to establish procedures for communicating security advisories and forwarding user-reported vulnerabilities.

HARMONIZED STANDARDS:

- Monitor the publication of harmonised standards.
- Identify which harmonised standards are relevant to your products (e.g., ETSI EN 303 645 for consumer IoT, EN IEC 62443-3-3 for industrial systems).
- Implement technical specifications from applicable harmonised standards to benefit from the presumption of conformity under Article 27.

EUROPEAN CERTIFICATION SCHEMES:

- Identify whether European cybersecurity certification schemes under the Cybersecurity Act are available and applicable to your products.
- Monitor the Commission's adoption of delegated acts specifying mandatory certification requirements for critical products.
- Engage with certification bodies early to understand scheme requirements, timelines, and costs.

HOW CAN WE ASSIST YOU?

BCLP's team is equipped to support your organization in navigating the compliance landscape introduced by the Cyber Resilience Act. We help identify products with digital elements impacted by the regulation through comprehensive gap analyses, assess product classification to determine applicable conformity assessment procedures, and assist in preparing technical documentation and EU declarations of conformity. Our guidance extends to the selection and implementation of appropriate conformity assessment routes, including engagement with notified bodies, application of harmonised standards, and evaluation of European cybersecurity certification schemes such as the EUCC.

We assist in drafting or revising contractual arrangements with suppliers, customers, distributors, and importers to ensure alignment with the CRA's requirements, including vulnerability disclosure obligations, security support commitments, and reporting responsibilities. Our support includes establishing robust vulnerability management and incident response procedures to meet the three-stage reporting requirements under Article 14, as well as developing internal policies for cybersecurity risk assessment and lifecycle management.

To support long-term compliance, we offer ongoing legal monitoring of delegated acts, implementing measures, and harmonised standards as they are adopted, and deliver tailored training sessions to in-house legal, technical, and product development teams, ensuring they remain informed and prepared.

By proactively addressing these obligations, manufacturers not only mitigate legal risk and avoid substantial penalties but also strengthen their competitive position in an increasingly security-conscious market, building customer trust through demonstrable cybersecurity commitment.

MEET THE TEAM

Pierre-Emmanuel Froge

Paris

pierreemmanuel.froge@bclplaw.com
+33 (0) 1 44 17 76 21
