Preparing for EU Cyber Resilience Act (CRA) Article 14 Compliance

Volume 8 | Issue 32 | Jun 2026
Author: Karl Lau, Tommy Leung; Proofread by Joey Kwok

Summary

- The European Union’s Cyber Resilience Act (CRA), Regulation (EU) 2024/2847, establishes the most stringent and comprehensive cybersecurity requirements ever applied to digital products entering the EU market. Among its provisions, Article 14—mandatory vulnerability and incident reporting—will take effect on 11 September 2026, leaving manufacturers with a limited window to implement compliant processes.
- This white paper outlines the CRA framework, highlights the critical compliance challenges introduced by Article 14, and introduces CMA Testing’s automated compliance solution, designed to enable organizations to meet reporting obligations efficiently, accurately, and at scale.

1. Overview of the EU Cyber Resilience Act (CRA)

The CRA is the EU's first horizontal cybersecurity regulation covering **all products with digital elements**. Its foundation is a unified principle:

"Security by design" combined with lifecycle cybersecurity assurance

Key Regulatory Objectives

- **Secure-by-design products**: No known exploitable vulnerabilities at market entry
- **Secure-by-default configurations**
- **Mandatory vulnerability management and free security updates**
- **Lifecycle cybersecurity responsibility**
- **Harmonized EU-wide compliance requirements**, eliminating fragmented national regulations

Scope of Coverage

The CRA applies broadly to:

- Hardware products
- Software applications
- Related remote data processing services (e.g., cloud-connected smart home systems)

2. Product Scope and Risk Classification

The CRA categorizes products into **three risk tiers**, covering nearly all digital products:

2.1 General Digital Products

All connected or digital-enabled products, including:

- Consumer electronics
- Office software
- Smart appliances

2.2 Important Products (Mandatory Third-Party Assessment)

Class I (Moderate Risk)

- Operating systems
- Routers
- Smart locks
- Password managers
- Smart cameras
- Wearable health devices
- Connected toys

Class II (High Risk)

- Firewalls
- Intrusion detection/prevention systems
- Hypervisors
- Container runtime systems
- Tamper-resistant processors and microcontrollers

2.3 Critical Products

- Hardware Security Modules (HSMs)
- Secure elements and chips
- Smart cards
- Smart meter gateways
- Advanced cryptographic devices

These products will require **EUCC certification under a unified EU framework**.

3. Responsible Economic Operators

The CRA imposes obligations across the full supply chain:

Stakeholder	Responsibility
Manufacturer	Design, testing, vulnerability management, security updates, lifecycle compliance
Importer	Verify CE marking and compliance documentation
Distributor	Ensure compliant products are sold; report risks
Private Label / Modifier	Assume full manufacturer responsibilities
Open Source Maintainers	Limited obligations (only for commercialized open-source products)

4. Consequences of Non-Compliance

Failure to meet CRA requirements can result in severe penalties:

- **Fines**: Up to **2.5% of global annual turnover** or **€15 million (whichever is higher)**
- **Market enforcement measures**:
  - Product bans
  - Mandatory recalls
  - Removal from EU markets
- **Additional consequences**:
  - Confiscation of illegal gains
  - Market access restrictions
  - Collective consumer lawsuits

5. Key Implementation Timeline

Date	Milestone	Urgency Level	Required Action
11 Sept 2026	Article 14 mandatory reporting enters into force	⭑ ⭑ ⭑ ⭑ ⭑	Deploy incident response and automated reporting systems
11 Dec 2027	Full CRA enforcement (CE marking mandatory)	⭑ ⭑ ⭑	Complete compliance certification for all products

6. Article 14: The Core Compliance Challenge

6.1 Mandatory Reporting Triggers

Manufacturers must report when:

- **Actively exploited vulnerabilities** are discovered
  - Evidence of real-world attacks or PoCs in circulation
- **Severe security incidents occur**, such as:
  - Malicious code injection
  - Large-scale data breaches
  - Device outages

6.2 Strict Reporting Deadlines

Deadline	Requirement
Within 24 hours	Early warning notification (to national CSIRTs and ENISA)
Within 72 hours	Detailed incident report (impact, scope, mitigation)
Within 14 days / 1 month	Final report (post-remediation or incident conclusion)

These timelines impose **extreme operational pressure**, particularly for globally distributed teams managing:

- Time zone differences
- Weekend incidents
- Language and regulatory reporting requirements

Even minor delays or inaccuracies can trigger **regulatory penalties or market withdrawal**.

7. CMA Testing: End-to-End Article 14 Compliance Solution

CMA Testing offers a **fully compliant, automated vulnerability reporting cloud service**, engineered to address the operational and technical challenges of Article 14.

7.1 SBOM Automation and Management

- Automatic generation or import of **Software Bill of Materials (SBOM)**
- Real-time linkage to global vulnerability databases
- Complete impact analysis across all components in **under 10 minutes**

7.2 Intelligent Filtering via VEX

- Integration of **Vulnerability Exploitability eXchange (VEX)**
- Automatically filters **60%+ false positives**
- Reduces reporting workload while maintaining compliance accuracy

7.3 AI-Powered Reporting Automation

- Built-in **AI compliance assistant**
- Auto-generates ENISA-compliant English reports in stages:
    - Early warning
    - Detailed report
    - Final report
- One-click human validation before **direct submission to ENISA platform**
- Designed to **meet 24h / 72h deadlines reliably**

7.4 End-to-End Visibility and Coordinated Disclosure

- Real-time dashboards for:
  - Compliance deadlines
  - Reporting status
- Integrated **Coordinated Vulnerability Disclosure (CVD)** portal:
  - Unified internal and external reporting entry point

7.5 Audit-Ready Compliance and 24/7 Monitoring

- Full activity logging for **regulatory traceability**
- Automated compliance record archiving
- **24/7 monitoring and alerting** to ensure zero reporting gaps

8. Additional CRA Compliance Requirements

Beyond Article 14, organizations must address ongoing obligations:

- ✓ **Minimum 5 years of free security updates** (longer for industrial products)
- ✓ Mandatory **SBOM generation and maintenance**
- ✓ Secure update requirements:
  - Automatic updates by default (consumer products)
  - Opt-out mechanisms for all products
- ✓ Clear **support lifecycle disclosure** and user notification
- ✓ Exposure to **consumer collective legal action** in case of violations

9. Conclusion: Immediate Action Required

The CRA’ s Article 14 represents a **zero-transition, zero-exemption requirement**. All digital products already on the EU market must comply by **11 September 2026**.

Organizations that fail to establish:

- Incident response mechanisms
- Automated vulnerability reporting
- Lifecycle security processes

will face **significant financial, operational, and reputational risks**, including market exclusion.