HCLTech | Supercharging Progress™

Cyber resilience by design

Navigating the EU CRA for products with digital elements

Table of contents

Disclaimer	3
Abstract	4
Terms and abbreviations	5
Introduction	7
Basics of CRA and legal context	7
Scope and applicability of the Cyber Resilience Act	9
Product classification under the CRA	10
Essential cybersecurity requirements	11
Compliance roadmap for manufacturers	13
Penalties and enforcement	14
HCLTech: Enabling end-to-end CRA compliance	15
Case Study: CRA compliance for a smart industrial connectivity device	16
Product overview	16
CRA applicability	16
Compliance product classification	16
Compliance strategy	17
Conclusion	18
References	18
Author information	20

Disclaimer

This whitepaper is produced by HCLTech for informational and awareness purposes only. It is intended to provide a general overview of the EU Cyber Resilience Act (Regulation (EU) 2024/2847) and does not constitute legal, regulatory or compliance advice. Regulatory interpretations, implementation guidance, harmonized standards, conformity assessment routes and enforcement practices may evolve as the CRA is operationalized across the European Union.

Manufacturers and other economic operators should consult official EU documentation, qualified legal counsel, notified bodies and relevant national market surveillance authorities before making decisions specific to their products, business context and applicable jurisdiction.

HCLTech makes no warranty, express or implied, regarding the completeness, accuracy or fitness for any particular purpose of the information contained in this document. HCLTech accepts no liability for any decisions made or actions taken based on the content of this whitepaper.

Abstract

The EU Cyber Resilience Act (CRA), Regulation (EU) 2024/2847, marks a significant shift in how cybersecurity is regulated for products with digital elements. It introduces mandatory cybersecurity requirements for hardware and software products with digital elements placed on the European Union market. The act represents a fundamental shift in product regulation: from voluntary cybersecurity guidance to binding legal obligations, with enforceable penalties and mandatory conformity assessment.

This whitepaper outlines the CRA's scope, legal context, product classification framework, essential cybersecurity requirements, compliance timelines, penalty structure and practical implications for manufacturers of industrial IoT and embedded systems. It provides a structured compliance roadmap aligned with recognized harmonized standards, including ETSI EN 303 645 [5] and the IEC 62443 series [6].

HCLTech supports manufacturers across the full CRA compliance lifecycle - from initial scope and gap analysis through secure-by-design integration, Software Bill of Materials (SBOM) management, coordinated vulnerability disclosure, conformity assessment readiness and ongoing post-market monitoring. Our Engineering and R&D Services practice, which includes an embedded device security capability, provides hands-on support to manufacturers seeking to meet CRA obligations while embedding security as a sustainable product-quality attribute.

Terms and abbreviations

Term	Full form	Description
ADCO	Administrative Cooperation Group	EU market surveillance authorities coordinating compliance enforcement across Member States.
CE	Conformité Européenne (European Conformity)	EU marking indicating that a product complies with applicable regulations and has completed the required conformity assessment.
CRA	Cyber Resilience Act	Regulation (EU) 2024/2847 — EU regulation establishing mandatory cybersecurity requirements for products with digital elements.
CSIRT	Computer Security Incident Response Team	National or sector-specific teams responsible for handling cybersecurity incidents and coordination.
CVD	Coordinated Vulnerability Disclosure	Process for identifying, reporting and responsibly addressing security vulnerabilities before public disclosure.
DoC	Declaration of Conformity	Manufacturer's formal written statement confirming that a product meets all applicable EU regulatory requirements.
ENISA	European Union Agency for Cybersecurity	EU body responsible for cybersecurity guidance, vulnerability coordination and supporting CRA implementation.
ETSI	European Telecommunications Standards Institute	Develops harmonised cybersecurity standards for IoT and PDEs, including ETSI EN 303 645.
EUCC	EU Common Criteria-based Cybersecurity Certification Scheme	EU cybersecurity certification scheme applicable to critical products under CRA Annex IV.
IEC	International Electrotechnical Commission	Global standards body for electrical and electronic systems, including IEC 62443 for industrial security.
IIoT	Industrial Internet of Things	Application of IoT technologies in industrial environments for automation, monitoring and efficiency.
IoT	Internet of Things	Network of interconnected physical devices that collect and exchange data via the internet or other networks.

ISO	International Organization for Standardization	Global standards body developing frameworks for quality, security and risk management.
NIS2	Network and Information Security Directive 2	EU directive (2022/2555) establishing cybersecurity obligations for entities in critical sectors.
OEM	Original Equipment Manufacturer	A company producing hardware or software components integrated into products sold by another manufacturer.
OS	Operating System	Software managing hardware resources and providing services for application programs.
PDE	Products with Digital Elements	Hardware or software products with direct or indirect connectivity to devices or networks, as defined by the CRA.
RED	Radio Equipment Directive	EU directive governing wireless communication devices; the CRA complements RED cybersecurity requirements.
SBOM	Software Bill of Materials	Machine-readable inventory of software components, dependencies and metadata enabling supply chain transparency.
SDL	Secure Development Lifecycle	Structured process integrating security requirements, design reviews, testing and governance throughout product development.
VPN	Virtual Private Network	Encrypted communication channel securing data transmission between endpoints over public networks.

Introduction

The digital transformation of industries has accelerated the adoption of connected devices, embedded systems, cloud-enabled applications and software-defined products.

This connectivity is creating new sources of value through automation, predictive analytics, remote monitoring and data-driven decision-making. At the same time, it is expanding the attack surface for manufacturers, operators and end users.

A vulnerability in a connected product is no longer a narrow product issue. In industrial environments, it can affect operational continuity, safety, data integrity, service availability and customer trust. As products become more software-intensive and ecosystem-dependent, cybersecurity must be treated as a core product-quality attribute rather than an after-market control.

Recognizing the growing cybersecurity risks, the European Union introduced the Cyber Resilience Act (CRA) – Regulation (EU) 2024/2847, to establish a common cybersecurity baseline for products with digital elements to remain secure throughout their lifecycle. **By 11 September 2026,** manufacturers must begin reporting vulnerabilities within 24 hours and by **11 December 2027,** full compliance with CRA requirements, including essential cybersecurity requirements, technical documentation, conformity assessment and CE marking, become applicable.

With enforcement deadlines approaching, EU-based manufacturers must act swiftly to integrate CRA requirements into their product development and compliance strategies to avoid penalties and market access restrictions.

Basics of CRA and legal context

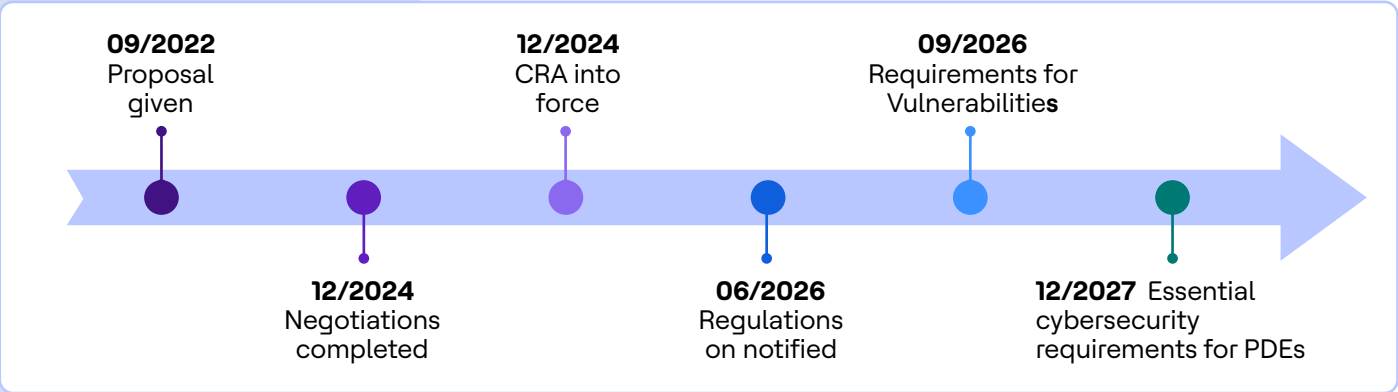
The **Cyber Resilience Act (CRA) [1]** was adopted by the European Parliament and the Council of the European Union on **23 October 2024** and published in the Official Journal of the European Union on **20 November 2024,**

CRA shall be enforced in two phases: phase 1 begins on **11 September 2026** with mandatory vulnerability reporting and phase 2 enforces full CRA compliance on **11 December 2027.** Here is the timeline.

Date	Key milestone
20 Nov 2024	CRA enters into force (published in the Official Journal of the EU)
11 Jun 2026	Notified bodies begin accepting conformity assessment applications.
11 Sep 2026	PHASE 1: Mandatory vulnerability and incident reporting obligations apply (Art. 14)

11 Dec 2026	Member States designate market surveillance authorities and CSIRT coordination points.
11 Dec 2027	PHASE 2: Full CRA compliance mandatory – all PDEs must bear CE marking before EU market placement

Table 1: Key milestones in the EU CRA implementation timeline (Regulation (EU) 2024/2847) [1]



The Act introduces horizontal cybersecurity requirements for hardware and software products that connect directly or indirectly to devices or networks. Its goals are to raise the baseline of product security, reduce vulnerabilities, provide clear support periods and align rules across the EU.

Key legislative highlights

- **Scope:** Applies to most products with digital elements, including connected consumer electronics, industrial control systems, embedded devices and software platforms with network connectivity. Products already regulated under sector-specific legislation (e.g., medical devices under EU 2017/745, automotive systems under EU 2019/2144, aviation and marine equipment) are excluded, as are defense and national security products.
- **Essential requirements:** Annex I defines product cybersecurity requirements (secure design, access control, data protection, resilience) and vulnerability handling (CVD, SBOM, patch management, incident reporting).
- **Conformity assessment:** Products must follow the appropriate conformity assessment procedure applicable to their risk category and bear the CE marking before EU market placement.
- **Reporting obligations:** Manufacturers must report actively exploited vulnerabilities within 24 hours and severe security incidents within 72 hours to ENISA [21] and designated CSIRTs [22].
- **Penalties:** Non-compliance may result in significant administrative fines of up to €15 million or 2.5% of global annual turnover, depending on the nature of the violation (Article 64) [1].

The CRA complements existing EU regulations such as the **NIS2 Directive[2], Cybersecurity Act (EU 2019/881)[3]** and **General Product Safety Regulation (EU 2023/988)[4],** creating a unified approach to cybersecurity governance market surveillance and product assurance across the EU single market.

Scope and applicability of the Cyber Resilience Act

The CRA applies to a wide range of products with digital elements (PDEs): hardware and software products that have direct or indirect data connections to devices or networks. This includes embedded systems, consumer electronic products, industrial control systems, software platforms and remote data processing solutions.

Scope of products under CRA

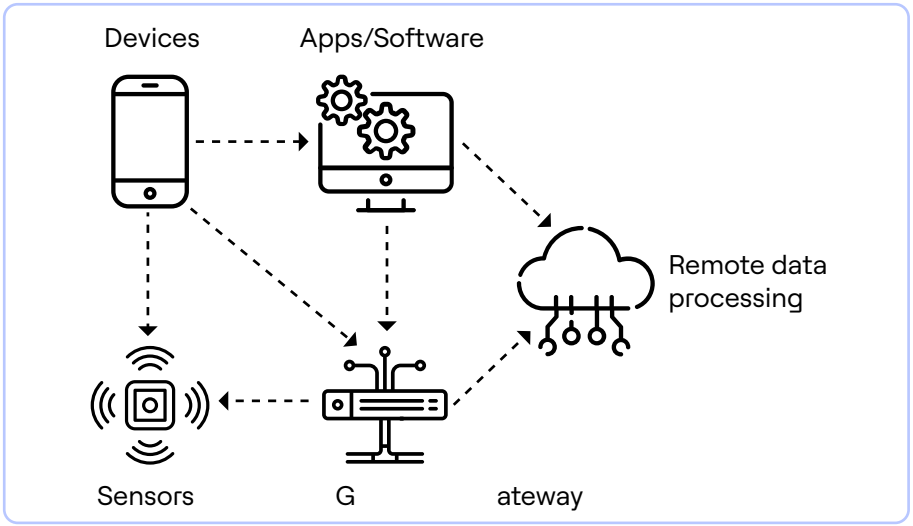


Figure 2 Representative Architecture of PDEs under the CRA

Category	Conformity assessment route	Certification / marking
PDEs	• Hardware and software with logical or physical data connections to devices or networks • Embedded systems • Consumer electronics • Industrial control systems	• Products regulated under sector-specific laws (medical devices, automotive, aviation, marine) • Defence and national security systems
Remote data processing	• Cloud-based services or mobile apps are essential for product functionality (e.g., smart scale using cloud analytics)	• General cloud services (SaaS, PaaS, IaaS) unless integral to product operation
Open-source software	• Included if integrated into a commercial product, the manufacturer is responsible for compliance	• Excluded if developed/ distributed outside commercial activity and not monetised
Examples	• Smart home devices (thermostats, door locks) • Industrial IoT devices (smart pumps, controllers) • Embedded systems in consumer electronics • Software platforms with network connectivity	• Medical devices (EU 2017/745, 2017/746) • Automotive systems (EU 2019/2144) • Civil aviation and marine equipment • Defence systems • Non-commercial open-source software

Table 2: CRA scope – Included and excluded product categories (Regulation (EU) 2024/2847, Articles 2 and 3) [1]

Implications for manufacturers

Manufacturers should treat scope assessment as a portfolio-level activity rather than a one-off product review. This helps identify common architectures, reusable evidence, shared third-party components and products that may require priority remediation.

Manufacturers are advised to:

- Confirm whether each product in the portfolio meets the definition of a PDE and is not covered by an applicable sectoral exclusion.
- Assess whether any remote data processing components (e.g., cloud services, mobile applications) are integral to product functionality and therefore in scope.
- Evaluate the cybersecurity obligations applicable to third-party software components, including open-source software incorporated into a commercial product.
- Maintain comprehensive technical documentation and committed support periods for all in-scope products.

Product classification under the CRA

The CRA introduces a risk-based classification framework for PDEs, that determines the applicable conformity assessment route before a product can be placed on the EU market. Classification depends on the cybersecurity risk profile of the product, its functionality and its potential downstream impact. The core categories are the default category, Important Products Class I, Important Products Class II and Critical Products.

Classification categories

Products are grouped into four categories as defined in Annexes III and IV:

Category	Representative examples	Conformity assessment route	Certification / marking
Default Category	Most connected products not listed in Annex III or IV (e.g., consumer smart devices, basic IoT sensors)	Self-assessment based on harmonized standards	EU Declaration of Conformity (DoC)
Important Products – Class I	Routers, modems, operating systems, network switches and identity management software	Self-assessment if harmonized standards are fully applied, otherwise third-party notified body assessment	DoC + possible third-party assessment
Important products– Class II	Firewalls, intrusion detection systems, hypervisors, tamper-resistant microprocessors	Mandatory third-party notified body assessment	Third-party assessment + CE marking
Critical products	Smart meter gateways, hardware security modules, secure elements (Annex IV)	EU cybersecurity certification (EUCC)at 'substantial' or higher assurance level	EUCC certification + CE marking

Table 3: CRA product classification and conformity assessment routes (Regulation (EU) 2024/2847, Annexes III and IV) [1]

Dynamic classification and delegated acts

The European Commission is empowered to amend Annexes III and IV via delegated acts to reflect technological evolution and emerging risks. Transitional periods include 12 months for changes to Annex III (Important Products) and 6 months for changes to Annex IV (Critical Products). Manufacturers should monitor Commission publications, ENISA guidance and harmonized standards to track classification changes that may affect their product portfolios.

Determining the correct classification

Product classification remains the manufacturer's responsibility and should be substantiated in the product's technical documentation.

The assessment should consider whether the product performs core cybersecurity functions, integrates security-relevant components, is deployed in a high-impact environment, or could create systemic risk if compromised.

- Core cybersecurity functionality, such as identity management, secure communication, access control or network protection.
- Incorporation of components such as firewalls, VPNs, hardware security modules, secure elements or tamper-resistant microprocessors.
- Intended use environment, including whether the product is deployed in consumer, enterprise, industrial, operational technology or critical infrastructure settings.
- Potential downstream impact of compromise, including safety, availability, data integrity and operational continuity implications.

Where classification is unclear, manufacturers should engage notified bodies, market surveillance authorities, legal advisors and technical specialists early enough to avoid delays during conformity assessment.

Essential cybersecurity requirements

Annex I of the CRA defines two groups of essential cybersecurity requirements that manufacturers must address throughout the product lifecycle.

Group I: Product cybersecurity requirements

Manufacturers must embed security into product design and development, production and delivery of products with digital elements. Annex I, Part I requirements include the following areas:

1. No known exploitable vulnerabilities: Products should be designed, developed and produced with due diligence so that they are free from known exploitable vulnerabilities at the time of market placement.
2. Secure-by-default configuration: Products should ship with secure defaults, protected administrative interfaces and unnecessary features disabled where possible.
3. Access control: Products must be protected against unauthorized access through appropriate authentication, authorization and identity management mechanisms.

4. Reduced attack surface: Exposed interfaces, services and attack vectors should be minimized through hardening, segmentation and secure interface design.
5. Data protection: Confidentiality and integrity of data at rest and in transit should be protected through appropriate cryptographic mechanisms.
6. Resilience against attacks: Products should be designed to maintain availability, resist denial-of-service conditions and operate in a degraded but secure state where appropriate.
7. Secure data removal: Products should enable secure deletion of user data and personal information.
8. Logging and monitoring: Products should provide security event logging and mechanisms to monitor anomalous behavior where appropriate.
9. Timely security updates: Products should support timely security updates, including automated update mechanisms where feasible and appropriate.

Figure 3 illustrates the essential cybersecurity requirements defined under the CRA Annex 1 for PDEs. It visually maps the key principles, such as secure by design, protection against unauthorized access and resilience against vulnerabilities. Left Flow (Preventive Measures) focuses on protection and minimizing risks, whereas right flow (Mitigation and Design) emphasizes secure design and response:

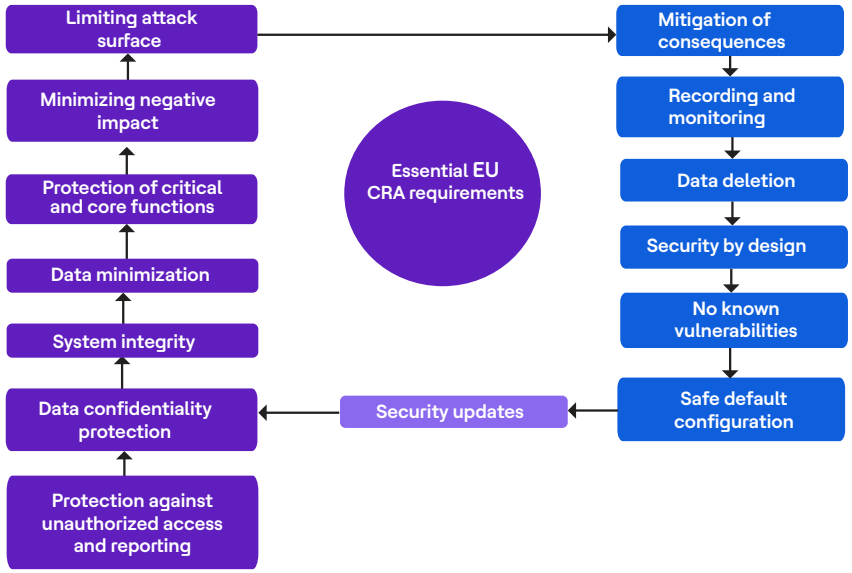


Figure 3 Essential cybersecurity requirements under the EU CRA

Group II: Vulnerability handling requirements

Annex I, Part II focuses on the processes and evidence required to handle vulnerabilities effectively throughout the declared support period. These obligations are central to lifecycle security and post-market resilience.

1. **SBOM:** Maintain a Software Bill of Materials in a commonly used, machine-readable format that identifies software components, dependencies and relevant version information.

2. **Coordinated Vulnerability Disclosure policy:** Publish and maintain

a CVD policy that enables responsible reporting by third-party researchers and other stakeholders.

3. **Security updates:** Provide timely and free security patches throughout the declared support period, while considering backward compatibility and operational continuity where feasible.

4. **Incident and vulnerability reporting:** Establish workflows to report actively exploited vulnerabilities and severe security incidents within the applicable CRA timelines.

5. **Technical documentation retention:** Retain technical documentation for the required period and keep it available for market surveillance authorities.

Product support period

Manufacturers must declare and commit to a minimum support period – the duration for which vulnerabilities must be handled effectively and security updates provided as required. The CRA establishes a minimum expected support period of five years or the reasonably expected product lifetime if shorter. For long-lived industrial products and critical infrastructure components, longer support periods may be necessary to ensure sustained security, operational resilience and customer trust.

Compliance roadmap for manufacturers

Achieving CRA compliance requires a phased, structured approach that integrates security into every stage of the product development lifecycle. The following roadmap provides a practical framework for manufacturers to meet CRA obligations while embedding security as a long-term product quality attribute.

Sr. no	Phase	Key actions	Key deadline
1	**Scope and portfolio analysis**	Identify all in-scope PDEs, verify exemptions, group products by category and reuse assessment strategies where possible.	Immediate
2	**Cybersecurity risk Assessment**	Evaluate product context, usage environment and potential attack paths. Document existing controls and identify gaps against Annex I requirements.	Immediate
3	**Secure design and development**	Integrate risk findings into product architecture. Apply harmonised standards (IEC 62443, ETSI EN 303 645). Continuously test and scan for vulnerabilities throughout SDL.	Ongoing
4	**Vulnerability handling setup**	Define the product support period (minimum five years). Establish secure update mechanisms, publish a CVD policy and maintain SBOM/HBOM. Implement reporting workflows for ENISA and CSIRTs.	By 11 Sep 2026
5	**Technical documentation**	Compile evidence package: product context, risk assessment outputs, SBOM/ HBOM, compliance evidence, support period declaration, update mechanisms description, contact details and instructions for users	Before market placement
6	**Conformity assessment and CE marking**	Issue EU Declaration of Conformity. Select self-assessment (Default/Class I with harmonised standards) or engage a notified body (Class II/Critical). Affix CE marking.	By 11 Dec 2027

Sr. no	Phase	Key actions	Key deadline
7	**Post-market monitoring**	Provide clear security instructions to users. Retain technical documentation for at least 10 years or the support period. Monitor regulatory updates and participate in market surveillance activities.	Ongoing

Table 4: Structured CRA compliance roadmap for product manufacturers

This roadmap helps manufacturers turn CRA compliance into a repeatable product security capability rather than a one-time regulatory exercise. The objective is to create a durable operating model that supports secure development, market access and sustained product resilience.

Penalties and enforcement

The CRA introduces significant administrative penalties for noncompliance. Penalties are set out in Article 64 of the Regulation [1] and may apply to manufacturers and other economic operators depending on the nature and severity of the violation.

Penalty structure

Key actions	Key deadline
Failure to meet essential requirements (Annex I)	By 11 Dec 2027 €15 million or 2.5% of global annual turnover
Breach of documentation, CE marking or conformity assessment obligations	€10 million or 2% of global annual turnover
Providing misleading or incomplete information to market surveillance authorities	€5 million or 1% of global annual turnover

Table 5: CRA penalty structure (Regulation (EU) 2024/2847, Article 64) [1]

Exemptions

The CRA provides limited penalty exemptions for specific categories of operators:

- Microenterprises and Small- and Medium-sized enterprises (SMEs) are exempt from administrative fines for failure to meet the 24-hour initial vulnerability reporting deadline, provided they report through the designated channels within a reasonable timeframe.
- Open-source software stewards acting in a non-commercial capacity are exempt from financial penalties, though they remain subject to certain notification and documentation obligations.

Enforcement mechanisms

Market surveillance authorities in each EU Member State are empowered under the CRA to:

- Restrict or prohibit the placement of non-compliant products on the EU market.
- Order the withdrawal or recall of products that present an unacceptable cybersecurity risk.
- Conduct joint investigations and coordinated market surveillance sweeps to identify systemic compliance issues.
- Refer cases to the European Commission for Union-wide corrective action where national measures are insufficient.

HCLTech: Enabling end-to-end CRA compliance

HCLTech empowers manufacturers to navigate the complexities of the EU CRA through a structured, end-to-end compliance enablement approach. Our Engineering and R&D Services practice, supported by embedded product security capabilities, combines deep domain expertise, regulatory interpretation, secure product engineering, lifecycle security and advanced automation tooling to accelerate CRA readiness while embedding security and resilience.

The goal is not only to help manufacturers meet regulatory obligations. It is to help embed cyber resilience into products by design, strengthen engineering governance, improve vulnerability visibility, accelerate conformity assessment readiness and build customer trust in connected products.

The following table summarises HCLTech's key CRA compliance service capabilities:

Sr. no	CRA compliance service	Description
1	**Cybersecurity risk Assessment**	Evaluate product portfolios to identify CRA applicability, risk exposure, product classification, compliance gaps and remediation priorities across the lifecycle.
2	**Secure-by-design integration**	Embed security principles into product architecture and development, aligned with relevant standards such as ETSI EN 303 645 and IEC 62443.
3	**SBOM management**	Generate, maintain and integrate SBOM and Hardware Bill of Materials evidence into the technical documentation and compliance package.
4	**Vulnerability disclosure and incident response**	Design CVD processes and incident reporting workflows aligned with ENISA, CSIRT and internal security operations requirements.
5	**Conformity assessment readiness**	Support product classification, technical documentation, evidence preparation, CE marking readiness and notified body engagement for applicable product PDEs.
6	**Secure update and patch management**	Implement secure update mechanisms, automated vulnerability scanning, patch governance and CI/CD security controls to sustain compliance post-launch.
7	**Training and awareness programmes**	Deliver tailored workshops for engineering, product, compliance, legal and supplier teams to build CRA-specific understanding and operating discipline.

Table 6: HCLTech CRA Compliance Service Capabilities

By leveraging these capabilities, HCLTech helps manufacturers transform CRA readiness from a compliance requirement into a strategic advantage: secure products, stronger resilience, faster market access and more transparent assurance for customers and regulators.

Case Study: CRA compliance for a smart industrial connectivity device

The following illustrative case study is based on a representative industrial IoT engagement. Product-specific details and client information have been anonymized and generalized to protect confidentiality. It is intended to demonstrate the compliance approach and methodology that HCLTech applies in an industrial IoT context.

Product overview

A Smart Industrial Connectivity Device (SICD) connects industrial pumps to the cloud via cellular and Ethernet interfaces, enabling remote monitoring, telemetry collection and predictive maintenance. The device includes embedded firmware, a local control interface and cloud connectivity components.

CRA applicability

- **In scope:** The SICD qualifies as a product with digital elements with direct and indirect data connections to networks and cloud services.
- **Not exempt:** The product is not covered by sector-specific regulations (e.g., medical devices, automotive systems) that would exclude it from CRA scope.4.3 Classification

CRA product classification

The SICD device falls under Important Product Class I or Class II, depending on a detailed technical assessment of the following factors:

- Whether the device performs core cybersecurity functions such as secure communications management, access control enforcement or VPN gateway functionality.
- Whether it incorporates security-relevant components such as hardware security modules, firewall capabilities or secure element chips.
- The potential impact of a security compromise on connected operational technology (OT) environments.

Classification was determined through a documented assessment process reviewed against Annexes III and IV, in consultation with the manufacturer's legal and compliance team.

Compliance strategy

Design and development

- Adopted secure-by-design principles and documented the product security architecture.
- Implemented secure boot, firmware integrity verification and role-based access control.
- Applied industry-standard cryptographic protocols, including TLS 1.3 or stronger where appropriate, for data transmission channels.
- Aligned engineering practices with IEC 62443-4-1 and ETSI EN 303 645 requirements.

Vulnerability management

- Generated and maintained a machine-readable SBOM for firmware and software components.
- Established a CVD policy with clear disclosure channels, response expectations and internal escalation workflows.
- Integrated automated vulnerability scanning, firmware update and patch management mechanisms into the product lifecycle.

Conformity assessment

- For a Class I pathway, prepared documented self-assessment evidence against applicable harmonized standards and internal control procedures.
- For a Class II pathway, prepared for notified body assessment by organizing product evidence, test results, risk assessments and technical documentation.

Documentation and marking

- Compiled a technical documentation package including product context, risk assessment, SBOM, test evidence, support period declaration and update mechanism description.
- Issued the EU Declaration of Conformity.
- Affixed the CE marking prior to EU market placement.

Incident reporting

Internal reporting processes were established to ensure compliance with CRA Article 14 reporting obligations:

- Actively exploited vulnerabilities: early warning within 24 hours, followed by full notification and final reporting in line with CRA timelines.
- Severe security incidents: early warning within 24 hours, full notification within 72 hours and final reporting within the required period.
- Internal governance: defined escalation owners, evidence capture, communication protocols and reporting readiness tests.

Conclusion

The EU CRA is reshaping product security governance across the EU market. It creates binding cybersecurity obligations for manufacturers of connected hardware and software and makes cyber resilience a prerequisite for market access, product trust and regulatory confidence.

Compliance requires more than documentation at the end of development. It requires a lifecycle-integrated operating model that starts with product scope and classification, continues through secure-by-design engineering and conformity assessment, and extends into vulnerability handling, patch management, technical documentation retention and post-market monitoring.

For manufacturers, the opportunity is to move beyond minimum compliance and use CRA readiness as a catalyst for stronger product assurance, improved supply chain transparency, faster response to vulnerabilities and more resilient customer outcomes.

HCLTech supports this transformation through its Engineering and R&D Services practice and embedded product security capabilities. From scope assessment and gap analysis through secure architecture, SBOM management, conformity assessment preparation and ongoing compliance maintenance, HCLTech helps manufacturers meet regulatory obligations while building trusted, resilient products for global markets.

References

1. Regulation (EU) 2024/2847 – Cyber Resilience Act. Official Journal of the European Union, 20 November 2024. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202402847
2. Directive (EU) 2022/2555 – NIS2 Directive on cybersecurity across the Union. Official Journal of the European Union.
3. Regulation (EU) 2019/881 – Cybersecurity Act on ENISA and ICT cybersecurity certification. Official Journal of the European Union.
4. Regulation (EU) 2023/988 – General Product Safety Regulation. Official Journal of the European Union.
5. ETSI EN 303 645 v2.1.1 – Cyber Security for Consumer Internet of Things: Baseline Requirements. European Telecommunications Standards Institute, 2020.
6. IEC 62443 Series – Industrial communication networks – Network and system security. Particularly IEC 62443-4-1 (Secure Development Lifecycle) and IEC 62443-4-2 (Technical security requirements for IACS components).
7. ISO/SAE 21434:2021 – Road vehicles – Cybersecurity engineering. International Organization for Standardization / SAE International.

8. ENISA – Cyber Resilience Act Requirements Standards Mapping. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/cyber-resilience-act-requirements-standards-mapping
9. Open Regulatory Compliance Working Group (ORCWG) – Getting Started With the CRA. https://orcwg.org/cra/
10. CRA-Ready.org – A Practical Guide to CRA Compliance. https://www.openappsec.io/post/cra-ready-org-a-practical-guide-to-cyber-resilience-act-cra-compliance
11. OpenSSF Tech Talk – CRA-Ready for Open Source Projects. https://openssf.org/blog/2025/06/16/cra-ready-how-open-source-projects-can-prepare-for-the-eu-cyber-resilience-act/
12. Digital SME Alliance – CRA and the Open-Source Community. https://www.digitalsme.eu/events/the-cyber-resilience-act-and-the-open-source-community/
13. Red Hat Blog – EU Cyber Resilience Act's Impact on Open Source Security. https://www.redhat.com/en/blog/eu-cyber-resilience-acts-impact-open-source-security
14. LPI.org – The Cyber Resilience Act and Open Source. https://www.lpi.org/blog/2025/09/09/the-cyber-resilience-act-and-open-source/
15. SBOM Generator – CRA SBOM Compliance Guide. https://sbomgenerator.com/compliance/eu-cyber-resilience-act
16. Cyber Resilience Act Explained. https://www.cyberresilienceact.eu/the-cra-explained/
17. CEN-CENELEC Webinar – Standards Supporting the CRA. March 2025. https://www.cencenelec.eu/media/CEN-CENELEC/Events/Webinars/2025/2025-03-10_webinar_cyberresilience_act.pdf
18. SGS Safeguards – Update on Developments Relating to the EU Cyber Resilience Act. September 2025. https://www.sgs.com/en-us/news/2025/09/safeguards-13125-update-on-developments-relating-to-the-eu-cyber-resilience-act
19. Digi International White Paper – Complying with the Cyber Resilience Act. https://hub.digi.com/dp/path=/marketing/asset/complying-with-the-cyber-resilience-act-cra-wp
20. Bureau Veritas – CRA Practical Guide v2.1. https://cybersecurity.bureauveritas.com/uploads/whitepapers/CRA-Practical-guide-ENG-2.1.pdf
21. ENISA – European Union Agency for Cybersecurity. https://www.enisa.europa.eu/
22. CSIRTs Network – EU CSIRT Coordination. https://csirtsnetwork.eu/

Author information

Yogesh Gupta

Yogesh is a product cybersecurity and compliance professional with more than 14 years of experience in secure product development, regulatory frameworks, and automotive and industrial IoT systems. As a Senior Technical Specialist at HCLTech, he leads strategic initiatives that help align product portfolios with emerging global cybersecurity regulations. Yogesh has supported OEMs and suppliers across industries including automotive, medical devices, consumer IoT and industrial automation. He has played a key role in interpreting and operationalizing the EU Cyber Resilience Act within industrial environments, particularly for connected devices and embedded systems. His work includes impact assessments, conformity strategies and internal learning sessions for cross-functional teams.

With expertise in standards and regulations such as ETSI EN 303 645, IEC 62443, ISO/SAE 21434, UNECE WP.29, the RED Delegated Act and the Australian Cyber Act 2024, Yogesh brings a practical, forward-looking perspective to cybersecurity compliance.

Yogesh is a member of HCLTech's Embedded Product Security Capability Unit within the Engineering and R&D Services organization. His work focuses on helping manufacturers meet regulatory obligations while building security and resilience into their digital products.

HCLTech | Supercharging Progress™

HCLTech is a global technology company, home to more than 223,000 people across 60 countries, delivering industry-leading capabilities centered around AI, digital, engineering, cloud and software, powered by a broad portfolio of technology services and products. We work with clients across all major verticals, providing industry solutions for Financial Services, Manufacturing, Life Sciences and Healthcare, Technology & Services, Semiconductor, Telecom and Media, Retail and CPG, Mobility and Public Services. Consolidated revenues as of 12 months ending June 2026 totaled $14.8B. To learn how we can supercharge progress for you, visit hcltech.com .

hcltech.com