

CONFORMVECTOR FIELD BRIEF

The Two CRA Deadlines US Industrial Manufacturers Need to Act On

A practical 2026-2027 product-engineering map for connected industrial products entering or already sold in the European Union.

11 Sep 2026**Article 14 reporting obligations apply****11 Dec 2027****Main CRA product obligations apply**

Why this brief exists

The Cyber Resilience Act is often presented as a 2027 compliance deadline. For manufacturers of connected products, that is incomplete. The reporting regime started earlier, while the 2027 obligations require evidence that is created inside product engineering: cybersecurity risk analysis, software-component visibility, vulnerability handling, support-period decisions, technical documentation and a defensible conformity route.

For a US manufacturer, the practical task is therefore not “write the CRA file in 2027.” It is “know which products and market routes are exposed, make reporting operational now where applicable, and build the evidence base before the product deadline.”

This field brief is written for industrial and embedded-product teams. It is technical orientation, not legal advice or certification.

1. Start with the product and the market route

The CRA applies to products with digital elements made available on the EU market where intended or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network, subject to defined exclusions and special regimes.

For US manufacturers, “we do not sell directly in Europe” is not a reliable scope test. Distributor, importer, OEM and white-label routes can still place a product on the EU market. The product and economic-operator roles should be mapped by route, not by the location of the sales contract.

Manufacturer role

A company that develops or manufactures a product - or has it designed or manufactured - and markets it under its own name or trademark can fall into the manufacturer role. White-label arrangements need particular attention: the brand and EU placement route can alter who carries manufacturer obligations for specific units.

Practical intake questions

- What does the product actually do, and what is its core functionality?
- Is it already made available in the EU, or is launch planned?
- Under whose name or trademark are units placed on the EU market?
- Are some units white-labelled by OEM partners?
- Do sector-specific exclusions or special regulations apply?

2. Deadline one: 11 September 2026

Article 14 reporting obligations apply from 11 September 2026. For products covered by the reporting regime and made available on the Union market, manufacturers need an operating process for actively exploited vulnerabilities and severe incidents affecting product security.

The key operational clocks

Trigger	Initial clock	Operational question
Actively exploited vulnerability	Early warning within 24 hours of awareness	Who decides reportability, who owns the clock, and who can submit?
Severe incident affecting product security	Early warning within 24 hours; main notification within 72 hours	Can engineering, product security and management escalate fast enough?

A normal incident-response policy is not automatically an Article 14 process. A defensible operating design identifies an accountable owner, reportability criteria, escalation routes, access to the Single Reporting Platform, clock handling, evidence capture and a tested workflow.

Pre-launch nuance

If a product has not yet been made available on the EU market, the reporting duty for that product route is not triggered merely because an EU launch is planned. But the process should be operational before launch; otherwise the first qualifying event can start the clock before the company has agreed who is responsible.

3. Deadline two: 11 December 2027

The broader CRA product obligations apply from 11 December 2027. By then, product teams need more than policies. They need a product-specific evidence chain that supports the security design, vulnerability handling, support decisions and conformity assessment.

The engineering evidence stack

Cybersecurity risk assessment

Product-specific risks, assumptions and intended/foreseeable use inform security requirements and controls.

Security requirements & traceability

Requirements link the identified risks to design controls, implementation and verification evidence.

SBOM

Machine-readable software component information covers at least top-level dependencies and remains tied to releases.

Vulnerability handling

Intake, triage, assessment, remediation, disclosure and tracking are documented across the support period.

Security updates

The organisation can deliver remediation, not merely produce firmware when convenient.

Support period

The security-support commitment is reasoned against expected product use; long-lived industrial products require explicit lifecycle thinking.

Technical documentation

Scope, classification, security evidence and conformity-route inputs are assembled in a reviewable product file.

4. Classification: why “has VPN” is the wrong shortcut

Important and critical product classification is not a feature-counting exercise. The product's core functionality is decisive. Integrating a secure bootloader, authentication component, operating system or VPN client does not automatically elevate the product as a whole.

Conversely, if the product itself has the core functionality described for an Annex III category - for example routing between separate networks, VPN functionality or network management - an Important Class I or II route may need to be assessed.

Example: two industrial gateways

Gateway A	Gateway B
Collects its own sensor data and publishes it to a configured cloud endpoint.	Routes arbitrary traffic between OT and IT networks and establishes VPN tunnels.
Default category may be plausible, subject to product review.	Important Class I may be likely, subject to product review and the applicable technical description.

Why Important Class I matters

Class I is not just a label. The conformity route changes. Internal control (Module A) is available only under the CRA conditions for applying relevant harmonised standards, common specifications or a qualifying European cybersecurity certification scheme. If those conditions are not met for the applicable requirements, a third-party conformity-assessment route is required.

5. Support period: the industrial-product trap

A support-period statement should not be evaluated only against a five-year number. The CRA requires the manufacturer to determine a support period that reflects expected product use, with a five-year baseline unless expected use is shorter. For industrial equipment that remains deployed for many years, the product-level rationale matters.

A common mismatch

Customer reality Machine or gateway remains in service for 10-15 years.	Supplier commitment Security updates promised for only 3-5 years.
---	---

That mismatch deserves explicit review. The answer may depend on product type, expected use, market communications and product-version lifecycle. The useful output is a documented rationale, not a generic statement that “five years is enough.”

Questions to resolve

- How long do customers reasonably keep the product in operational use?
- From what point is the support commitment measured for units placed on the market?
- Can security updates or other remediation be delivered across that period?
- What happens to late-sold units and long-lived installed bases?
- Is the support-period rationale reflected consistently in customer-facing documentation?

6. A practical 90-day readiness sequence

Priority	0-30 days	30-60 days	60-90 days
Market & roles	Map EU routes, OEM/white-label cases and product families.	Confirm manufacturer/importer/distributor roles.	Freeze assumptions used for conformity planning.
Article 14	Assign owner; define clocks and criteria; gain SRP access.	Run tabletop; connect vulnerability intake to reporting decision.	Close issues and formalise evidence of readiness.
Product evidence	Inventory existing cyber-risk, SBOM, update and support evidence.	Build missing risk traceability and CVD/vulnerability procedures.	Assemble technical-documentation inputs and verification evidence.
Classification	Triage core functionality against Annex III/IV descriptions.	Document likely class and assumptions.	Select conformity route and identify external assessment need, if any.

The objective is not to “finish CRA” in 90 days. It is to turn an ambiguous regulatory deadline into a product-specific engineering plan: defined scope, defensible classification, operating reporting process, known evidence gaps and an executable sequence to close them.

7. What a product-readiness assessment should leave behind

Applicability and role memo

Which product family, market routes and economic-operator roles were assessed; what assumptions remain open.

Classification reasoning

A product-level argument tied to core functionality and the current technical descriptions.

Article 14 readiness review

Owner, decision criteria, escalation, clocks, SRP access and tested workflow.

Annex I evidence-gap matrix

A traceable picture of risk, requirements, SBOM, vulnerability handling, update capability and supporting evidence.

Support-period review

Expected use compared with the stated security-support commitment and lifecycle rationale.

Prioritized remediation plan

A short, sequenced list of actions with evidence targets - not a generic backlog.

ConformVector uses the free CRA QuickCheck as preliminary triage. The paid CRA Product Readiness Assessment converts those signals into documented product-level reasoning and a 90-day plan for one product family.

conformvector.com/quickcheck/ | conformvector.com/assessment/

8. Primary references

Regulation (EU) 2024/2847 - Cyber Resilience Act

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R2847>

European Commission - CRA reporting obligations

<https://digital-strategy.ec.europa.eu/en/policies/cra-reporting>

Commission Implementing Regulation (EU) 2025/2392 - technical descriptions for important and critical products

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32025R2392>

European Commission - Cyber Resilience Act implementation

<https://digital-strategy.ec.europa.eu/en/factpages/cyber-resilience-act-implementation>

About ConformVector

ConformVector provides EU product-compliance engineering for US manufacturers of industrial, embedded and connected products. The work is led by Ronald Reisener, Dipl.-Inf. (FH), with more than 20 years of experience across embedded systems, requirements-based engineering, medical technology, avionics and system integration.

This document is a practical engineering brief, not legal advice, certification, notified-body activity or an official conformity decision. Product scope, classification and conformity route remain product-specific.