

SAMPLE DELIVERABLE

# CRA Product Readiness Assessment

Fictional product example - redacted-style excerpt showing the form of a ConformVector assessment package.

|                                                                      |                                                                                   |
|----------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| <b>Sample product</b><br>CVX-420 Industrial Edge Gateway (fictional) | <b>Assessment scope</b><br>One product family; US manufacturer; planned EU launch |
|----------------------------------------------------------------------|-----------------------------------------------------------------------------------|

## Executive readiness snapshot

| Signal                   | Assessment signal        | Why it matters                                                                                                |
|--------------------------|--------------------------|---------------------------------------------------------------------------------------------------------------|
| EU market exposure       | PLANNED                  | EU launch would bring the product and manufacturer route into CRA scope analysis.                             |
| Article 14 readiness     | PRE-LAUNCH GAP           | No named owner or tested 24h/72h reporting workflow is yet in place.                                          |
| 2027 evidence foundation | PARTIAL                  | SBOM and penetration testing exist; product-specific cyber-risk traceability and CVD evidence are incomplete. |
| Support period           | HIGH-PRIORITY REVIEW     | Current security-update commitment is 5 years; expected operational use is 10-15 years.                       |
| Classification           | LIKELY IMPORTANT CLASS I | Routing between OT/IT networks and VPN tunnelling are described as core product functions.                    |

## Executive finding

The product appears to have a credible EU market path, but the evidence and lifecycle commitments are not yet aligned to that path. The two highest-priority items are (1) establishing Article 14 reporting readiness before EU placement and (2) resolving the mismatch between expected field life and the stated security-support period. Classification should be treated as an Important Class I working hypothesis until confirmed against the final product configuration and applicable technical descriptions.

**Important:** This sample is illustrative only. It is not a CRA legal opinion, certification result, or statement about any real product.

## 2. Classification reasoning excerpt

### Product facts used

- Device sits between an OT network and an IT/cloud environment.
- Routing and packet forwarding between separate networks are described as core functions, not incidental communications.
- The device establishes VPN tunnels for secure remote connectivity.
- Firewall rules are ancillary; the product is not positioned primarily as IDS/IPS, SIEM or identity-management software.
- A subset is supplied white-label to OEM partners and must be reviewed by market route and branding.

### Preliminary classification signal

**Likely Important Class I.** The stated core routing function plausibly matches the CRA Annex III router category; VPN functionality is also separately listed. Final classification remains product-specific and should be documented against the applicable technical descriptions.

### Conformity-route consequence

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

### White-label route

Where an OEM places white-labelled units on the EU market under its own name or trademark, that route needs a separate manufacturer-role assessment. The supplier and OEM should not assume that one company's CRA evidence package automatically resolves the other company's obligations.

### Gap-matrix excerpt

| Area           | Evidence observed                 | Signal             | Next evidence target                                                                   |
|----------------|-----------------------------------|--------------------|----------------------------------------------------------------------------------------|
| Article 14     | General incident-response process | Gap signal         | Named owner; reportability criteria; tested 24h/72h workflow; SRP submission readiness |
| Cyber risk     | General security requirements     | Partial            | Product-specific cybersecurity risk assessment linked to requirements and controls     |
| SBOM           | CycloneDX per release             | Stronger           | Verify variant coverage, firmware components and release traceability                  |
| CVD            | security@ address                 | Partial            | Published coordinated-vulnerability-disclosure policy and contact route                |
| Support        | 5-year security updates           | High priority      | Document expected-use rationale and revise commitment for 10-15-year field life        |
| Classification | Router/VPN core functions         | Important I likely | Formal product-level classification memo with assumptions and cited criteria           |

### 3. Prioritized 90-day remediation plan excerpt

| Window     | Workstream                         | Outcome / evidence target                                                                                                          |
|------------|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| 0-30 days  | Article 14 operating process       | Assign accountable owner; define decision criteria and escalation; document 24h/72h workflow; run tabletop exercise.               |
| 0-30 days  | Classification & market-route memo | Confirm Important Class I hypothesis; map direct sales, distributor routes and white-label OEM cases separately.                   |
| 0-45 days  | Support-period decision            | Document expected use; align security-support commitment and customer-facing lifecycle language.                                   |
| 30-60 days | Cyber-risk traceability            | Create product-specific cybersecurity risk assessment and link risks to security requirements, controls and verification evidence. |
| 30-60 days | CVD & vulnerability handling       | Publish CVD policy; define intake, triage, remediation and communication criteria; tie to Article 14 decision path.                |
| 45-90 days | Conformity evidence package        | Close priority Annex I evidence gaps; assemble technical documentation inputs for the selected conformity route.                   |

#### What the full package adds

The paid assessment expands this excerpt into a documented product and market-route scope, classification reasoning with assumptions, Article 14 readiness review, Annex I evidence-gap matrix, support-period rationale, prioritized remediation actions and a review call. Missing evidence is treated as a finding, not as a reason to stop the review.

Typical engagement: one product family, fixed scope, target seven business days subject to timely intake.