KROLL®

# The Kroll Cyber Resilience Act Framework

A 62-control framework built for the product layer, not bolted onto the organizational one. This preview sets out the eight domains, their regulatory weighting, the maturity model, where your existing certifications carry you, and where they run out.

**62 Controls**
Eight weighted domains

**0–5 Maturity**
Not pass / fail

**CRA-Mapped**
Annex I, II & Arts. 13–28

WHY A CRA-SPECIFIC FRAMEWORK

# Your certificates are an asset, not a shortcut

Every security leader we work with already runs a credible program. Most hold ISO 27001, many align to NIST CSF 2.0, and a few have layered in IEC 62443 or NIST SSDF for product engineering. The natural assumption is that those certifications carry a manufacturer most of the way to CRA conformity. In our experience, they do not.

The reason is a difference in what is being governed. Existing frameworks describe how an **organization** manages security. The CRA describes how a **product** behaves once it is placed on the market. That single distinction changes who is accountable, what evidence is required and where the audit ultimately lands.

> **What we see in the field.** A connected multifunction-printer manufacturer we advised this year held ISO 27001 across three sites and ran a mature software development life cycle. Its remaining gap to CRA readiness still came to roughly nine months of net-new work, almost none of it visible through the enterprise security program. That pattern repeats across sectors, which is exactly why the framework had to be built for the product layer.

The CRA is, at its core, a product-engineering regulation written in the language of compliance. Treating it purely as a governance exercise is the fastest route to failing a conformity assessment. The framework in this preview keeps the emphasis in line with the regulation, on how the product behaves, how it is maintained and is reported on across its supported life.

THE FRAMEWORK AT A GLANCE

# Eight domains, weighted where the regulation looks

The framework consists of 62 controls structured across eight domains, drawn directly from CRA Annex I, Annex II and Articles 13 to 28. Each domain is weighted by where the regulation places its emphasis, not by where security teams tend to be most comfortable.

| CODE | DOMAIN | WEIGHT |
|---|---|---|
| PS | Product Security Design | 25% |
| VM | Vulnerability Management | 20% |
| IR | Incident Response and ENISA Reporting | 15% |
| TD | Technical Documentation | 10% |
| CA | Conformity Assessment | 10% |
| SC | Supply Chain Security | 8% |
| PM | Post-Market Surveillance | 7% |
| OG | Organizational Governance | 5% |

**Product security design and vulnerability management together carry 45%.** That is deliberate. The CRA rewards manufacturers who can prove how the product behaves and how vulnerabilities are handled per product.

HOW WE SCORE

# A 0–5 maturity model, not a pass/fail tick box

A binary scoring method does not work for true readiness. Manufacturers need to know where they sit on the curve, what good looks like for their product class, and how much runway remains to close the gap. Every control is scored on a six-point scale, with **Level 3 (defined)** as the working target for CRA conformity and **Level 4 (managed and measurable)** for Class II and Critical product families.

| | |
|---|---|
| 0 | **No Capability**<br>No process, evidence or ownership. The requirement is not addressed. |
| 1 | **Initial**<br>Ad hoc and reactive. Isolated activity that depends on individuals, not process. |
| 2 | **Repeatable**<br>A basic process exists but is inconsistent and lightly documented across products. |
| 3 | **Defined** — CONFORMITY TARGET<br>Documented, standardized and applied per product. The working target for CRA conformity. |
| 4 | **Managed and Measurable**<br>Metrics-driven and monitored. The target for Class II and Critical product families. |
| 5 | **Optimizing**<br>Continuously improved with feedback loops feeding design and engineering. |

**Why does this matters operationally?** A manufacturer at Level 2 in vulnerability management can still ship in 2026 if it holds a credible plan to reach Level 3 by mid-2027. A manufacturer at Level 1 with no SBOM and no disclosure process cannot. The maturity model draws that line clearly, whereas a red/green dashboard does not.

WHERE THE CERTIFICATES HELP

# 92% coverage and five controls no framework touches

We mapped all 62 controls against five widely adopted frameworks. Holding ISO/IEC 27001:2022 together with NIST CSF 2.0 gives a manufacturer roughly 92% topical coverage of the CRA. The catch sits in the remaining five controls that are not covered.

**36**
Controls map **directly** to ISO 27001 + NIST CSF 2.0

**21**
Controls map **partially,** topically close, operationally different

**5**
Controls with **no equivalent** in any security framework

| DOMAIN | SAMPLE CONTROL THEME | ISO 27001 + NIST CSF 2.0 |
|---|---|---|
| **PS** Product Security | Secure-by-default configuration | Direct |
| **VM** Vulnerability Mgmt. | Per-product SBOM & coordinated disclosure | Partial |
| **IR** Incident / ENISA | 24h / 72h / 14d reporting to CSIRT and ENISA | Partial |
| **CA** Conformity | Product classification and CE marking procedure | No equivalent |
| **CA** Conformity | Declaration of Conformity and Notified Body | No equivalent |
| **TD** Technical Docs | Annex VII technical file compilation | No equivalent |

**The five uncovered controls are the conformity-assessment controls (CA.1–CA.7 plus TD.7).** They sit at the regulatory core of the CRA and are product-safety regulation, borrowed from the world of CE marking on machinery and toys. Closing them needs legal, regulatory affairs and product engineering working together, and a security team cannot close them alone.

A note of caution on the 21 partial mappings: they create the falsest confidence. ISO 27001 covers vulnerability management at the organizational level; the CRA requires it per product, with mandatory coordinated disclosure, a public contact point and machine-readable advisories per product family.

NEXT STEP

# See where your products sit on the curve

This preview is an extract of the same 62-control artefact we use in client kick-offs. The full walkthrough scores your product families, assigns gap severity against fixed remediation windows and turns the output directly into a budgeted program plan.

- ✓ **Reporting readiness** for the 11 September 2026 CSIRT and ENISA obligation
- ✓ **SBOM and vulnerability handling** assessed per product, not per organization
- ✓ **Conformity-assessment path** and Notified Body engagement planned early
- ✓ **A defensible roadmap** to arrive audit-ready, not audit-hopeful, by December 2027

**Book a framework walkthrough with our advisory team:**

**Hristiyan Lazarov** Associate Managing Director, Cyber Risk
**Craig Parkin** · **Tiernan Connolly** Cyber Risk Advisory

Kroll's Cyber Risk Advisory team supports connected-product manufacturers across the EU on CRA readiness, conformity-assessment preparation and ENISA reporting operations. This document is provided for general information only and does not constitute legal or regulatory advice. Regulation (EU) 2024/2847 and its implementing acts should be consulted directly. 