PENTESTERRA

CYBER RESILIENCE ACT GAP ASSESSMENT

Are Your Digital Products Ready for the CRA?

Gap assessment across 24 Cyber Resilience Act controls - security-by-design and vulnerability-handling requirements - for manufacturers of hardware and software sold in the EU.

IN SHORT

Covers the essential cybersecurity and vulnerability-handling requirements in Annex I of the CRA. Reporting obligations to ENISA/CSIRT apply from 11 September 2026, essential requirements from 11 December 2027 - the design-and-process work (SBOM, CVD policy, update mechanism) takes real lead time.

24
CRA controls covered (Annex I)

2027
Deadline for essential cybersecurity requirements

EU-Wide
Manufacturers of products with digital elements

THE SITUATION TODAY

WHO YOU ARE

You're the product or security lead of a company manufacturing hardware or software with digital elements for the EU market, preparing for Cyber Resilience Act obligations.

WHAT HAPPENED

CRA deadlines are approaching (2026 for reporting, 2027 for essential requirements), and SBOM, vulnerability-disclosure policy, and update mechanism aren't structured yet.

WHY IT HURTS

CRA requirements need design-and-process work that can't be improvised close to the deadline - SBOM and vulnerability handling have to be built into the product, not bolted on afterward.

WHERE YOU WANT TO GET TO

DESIRED OUTCOME	You want to know, control by control, what's satisfied, what's partial, and what's missing - with real technical evidence attached to every answer, not an optimistic claim nobody has verified.
THE SOLUTION	Pentesterra's Cyber Resilience Act Gap Assessment: a structured assessment across every control, with technical controls auto-filled from vulnerability scanning, penetration testing, OSINT and External Exposure monitoring wherever evidence exists.
WHY IT'S DIFFERENT	You're not buying another self-assessment questionnaire, and this isn't a legal opinion. You're working with [YOUR COMPANY NAME] - a certified provider with a long track record in information security. You've likely worked with us already, directly or through someone you know - a colleague, a supplier, a competitor. And the gap assessment doesn't stop at a paper checklist: technical controls are auto-filled from evidence already on file, with cross-standard mapping to the other 12 frameworks the platform supports, so a second audit never starts from zero.
CONCRETE PROOF	The result is a complete, ready-to-deliver PDF report covering every control, with a direct reference to the legal/regulatory basis. If gaps come up, we propose the additional services to close them: vulnerability assessment, network or application penetration testing, phishing training and simulation.

WHAT'S ACTUALLY INCLUDED

Not a generic checklist - the real controls of Cyber Resilience Act, grouped the way you'll see them in the platform.

Annex I Part I: Security by design

The essential cybersecurity requirements of the product.

- No known exploitable vulnerabilities at delivery
- Secure by default configuration
- Protection of data processed by the product

Annex I Part II: Vulnerability handling

The process that continues after the product ships.

- Identification and documentation of components (SBOM)
- Vulnerability handling and remediation
- Secure update mechanism

Art. 11 reporting and Art. 13 documentation

The obligations toward ENISA/CSIRT and technical documentation.

- Reporting of actively exploited vulnerabilities
- Reporting of incidents with a security impact
- Technical documentation of the product

Getting ready for the 2026-2027 deadlines

The design work takes real lead time, it can't be improvised.

- Roadmap to compliance by December 2027
- Gap assessment on existing SBOM and CVD policy
- Prioritization of the highest-risk components

WHAT YOU GET

- ✓ An exportable XLSX control matrix, with the status of every individual control
- ✓ An editable DOCX gap report, ready for your auditor or your board
- ✓ Technical controls auto-filled from evidence the platform already collected
- ✓ Guided applicability check by sector, country, and company size
- ✓ Cross-standard mapping to the other 12 frameworks the platform supports - answer once, reuse across standards
- ✓ A one-click auditor package: questionnaire, technical evidence and gap report together
- ✓ Prioritized remediation recommendations for the gaps found

HOW IT WORKS

1

We define the scope

Assessment boundary, systems and processes involved - we set the scope together.

2

We collect the evidence

Technical controls are auto-filled from evidence the platform already collected.

3

We complete the questionnaire

Non-technical controls are verified with your team.

4

We deliver the report

A complete PDF with the gaps found and the actions to take.

Find out how ready you are for Cyber Resilience Act

A complete report, ready to present to clients, auditors, or your board.

Request your Cyber Resilience Act Gap Assessment →

info@pentesterra.com · pentesterra.com/solutions/compliance