VCRI
THE VALUE CHAIN RISK INSTITUTE

VCRI LEARN · EU CYBER RESILIENCE ACT

The EU Cyber Resilience Act in 10 minutes

What it covers, what it asks of you, the dates that matter, and what to do now.

Joshua Marpet and Cairn Viktor

VCRI
THE VALUE CHAIN RISK INSTITUTE

WHY DO I CARE

If you sell software or connected things in the EU, this is yours

It is already live

Since 11 September 2026, manufacturers must report actively exploited vulnerabilities.

That includes products already on the EU market.

It reaches US companies

It applies to products made available on the EU market, wherever they were built.

EU importers may only place compliant products on the market.

It has teeth

Breaking the core requirements can cost up to EUR 15 million or 2.5% of worldwide annual turnover, whichever is higher.

Sources: Regulation (EU) 2024/2847 Art. 2, 19, 64, 71; European Commission CRA reporting page; Ireland NCSC CRA page.

valuechainrisk.org/learn · CC BY 4.0

VCRI
THE VALUE CHAIN RISK INSTITUTE

WHAT IT COVERS

Products with digital elements

In scope

Software or hardware, plus the remote data processing it needs to work, that connects directly or indirectly to a device or network.

Examples the Commission gives: baby monitors, smart watches, apps, computer programs.

Outside it

Products already covered by their own EU rules: medical devices, in vitro diagnostics, vehicles, certified aviation products, marine equipment.

National security and defence products. Open source that is not supplied in a commercial activity.

Sources: Regulation (EU) 2024/2847 Art. 2 and 3(1), recitals 18 and 26; European Commission CRA policy and summary pages.

valuechainrisk.org/learn · CC BY 4.0

VCRI
THE VALUE CHAIN RISK INSTITUTE

THE BIG IDEA

Security for the whole life of the product

Design

Assess the cybersecurity risk. Ship with no known exploitable vulnerabilities and a secure by default configuration.

→

Ship

Technical documentation, conformity assessment, CE marking, and user instructions that state the support end date.

→

Support

Handle vulnerabilities for the support period: at least five years, or the expected use time if shorter.

→

Report

Tell the authorities fast when a vulnerability in your product is being actively exploited.

Sources: Regulation (EU) 2024/2847 Art. 13, 14, Annex I, Annex II; European Commission CRA summary page.

valuechainrisk.org/learn · CC BY 4.0

KEY OBLIGATIONS

Five things engineers will actually do

Secure by design

Build to the Annex I essential requirements, based on a written risk assessment.

Secure by default settings, with a way to reset to the original state.

Vulnerability handling

A coordinated vulnerability disclosure policy and a public contact point.

Fix without delay and publish advisories once a fix ships.

SBOM

A software bill of materials (SBOM): a machine-readable list of what is inside your product, at least the top-level dependencies.

Security updates

Free of charge, with advisory messages. Each update stays available for at least 10 years or the rest of the support period, whichever is longer.

Plus the fifth: report actively exploited vulnerabilities. Next slide.

Sources: Regulation (EU) 2024/2847 Art. 13(8)-(9), Annex I Parts I and II.

valuechainrisk.org/learn · CC BY 4.0

VCRI
THE VALUE CHAIN RISK INSTITUTE

REPORTING

The clock starts when you become aware

Reported once, through the CRA Single Reporting Platform, to the national CSIRT (computer security incident response team), with ENISA (the EU cybersecurity agency) informed.

24 hours
Early warning of an actively exploited vulnerability or a severe incident.

→

72 hours
Full notification with more detail.

→

Final report
Within 14 days after a fix is available (vulnerabilities), or within one month (severe incidents).

Sources: European Commission CRA reporting and summary pages; Regulation (EU) 2024/2847 Art. 14.

valuechainrisk.org/learn · CC BY 4.0

KEY DATES

Four dates to put on the wall

DATE	WHAT HAPPENS
10 December 2024	The CRA entered into force.
11 June 2026	Rules for conformity assessment bodies (notified bodies) apply.
11 September 2026	Reporting of actively exploited vulnerabilities and severe incidents applies.
11 December 2027	The main obligations apply: essential requirements, conformity assessment, CE marking.

Sources: Regulation (EU) 2024/2847 Art. 71(2); European Commission CRA policy page (updated 7 September 2026) and summary page.

valuechainrisk.org/learn · CC BY 4.0

VCRI
THE VALUE CHAIN RISK INSTITUTE

PRODUCT CATEGORIES

Riskier products get a stricter check

CATEGORY	EXAMPLES FROM THE ANNEXES	HOW CONFORMITY IS SHOWN
Default	Everything not listed in Annex III or IV	Self-assessment by the manufacturer
Important, Class I	Browsers, password managers, VPNs, operating systems, routers, smart home security products	Self-assessment only if harmonised standards or a certification scheme are applied; otherwise a notified body
Important, Class II	Hypervisors, firewalls, intrusion detection, tamper-resistant microcontrollers	Third-party assessment
Critical	Hardware devices with security boxes, smart meter gateways, smartcards	Third-party assessment or a European certification scheme

Sources: Regulation (EU) 2024/2847 Annex III and Annex IV; European Commission CRA summary page.

valuechainrisk.org/learn · CC BY 4.0

VCRI
THE VALUE CHAIN RISK INSTITUTE

WHAT TO DO MONDAY

Five steps you can start this week

- Find out if you are in scope: do you sell a product with digital elements in the EU, directly or through importers and distributors?
- Name your reporting owner and rehearse a 24 hour early warning. This duty is live now.
- Generate an SBOM for every shipping product and keep it current with each release.
- Decide and write down your support period, and publish a coordinated vulnerability disclosure policy with a contact point.
- Start the risk assessment and the user security information now. December 2027 is closer than it looks.

valuechainrisk.org/learn · CC BY 4.0

FREE TOOLS

Three free VCRI tools for the paperwork

All run in your browser. Nothing is uploaded.

CRA Manual Builder

Write the user security manual the CRA requires (Annex II) on the Cyber Manual Movement template. Import an SBOM; export JSON or PDF.

valuechainrisk.org/cra-manual-builder

Context & Conditions of Use Builder

Derive context components, persons and zones from your product's functions, attach conditions of use, and get the diagrams from one picture.

valuechainrisk.org/cyber-manual/context

CRA TARA Builder

Build the cybersecurity risk assessment (Annex VII) as a companion to the manual, and feed accepted risks back into it.

valuechainrisk.org/tara

Source: valuechainrisk.org/tools. The template is the Cyber Manual Movement working group's; it has not reviewed these tools.

valuechainrisk.org/learn · CC BY 4.0

READ THIS FIRST

This deck is not legal advice

It is a teaching summary of Regulation (EU) 2024/2847 as of October 2026. Whether and how the CRA applies to your product depends on facts we do not know. Read the official text on EUR-Lex and the European Commission's CRA pages, and talk to qualified counsel before you rely on any of it.

valuechainrisk.org/learn · CC BY 4.0

VCRI

THE VALUE CHAIN
RISK INSTITUTE

Free to use, teach and share.

This deck is part of the VCRI Learn series. Use it in your class, your team meeting or your chapter, with credit to The Value Chain Risk Institute.

valuechainrisk.org/learn

valuechainrisk.org/learn · CC BY 4.0