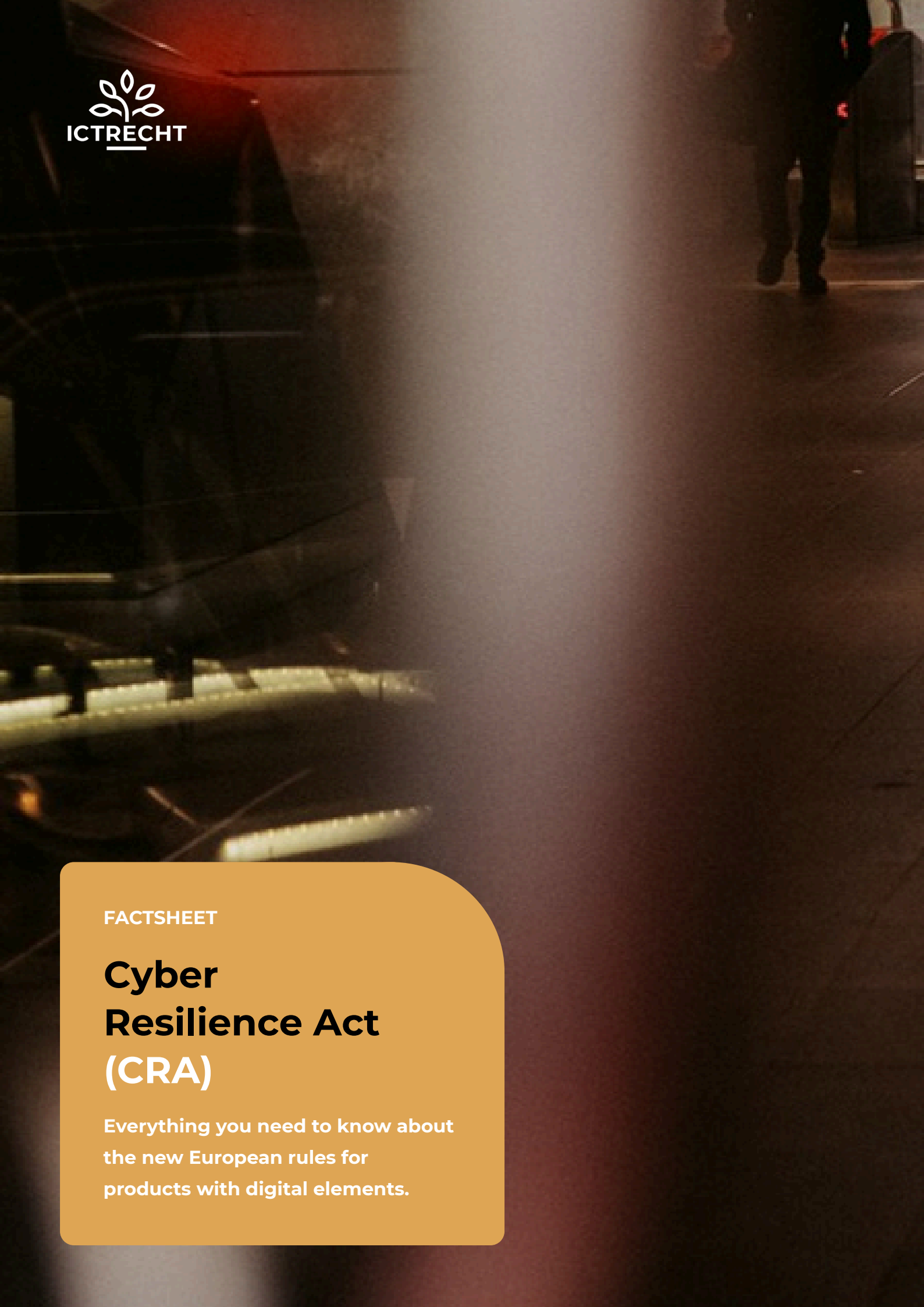


ICTRECHT

FACTSHEET

Cyber Resilience Act (CRA)

Everything you need to know about the new European rules for products with digital elements.

What is the Cyber Resilience Act (CRA)?

The Cyber Resilience Act (Regulation (EU) 2024/2847) is a European regulation that sets cybersecurity requirements for **products with digital elements** offered on the EU market. The regulation entered into force on 10 December 2024.

The CRA applies to virtually all hardware and software that is connected, or can be connected, to the internet or a comparable digital network. This includes smart devices such as TVs, doorbells and baby monitors, as well as smartphones, smartwatches, laptops, tablets, e-readers, and all software installed or installable on them.

Four pillars of the CRA

Safer products

fewer vulnerabilities at market introduction.

Lifecycle approach

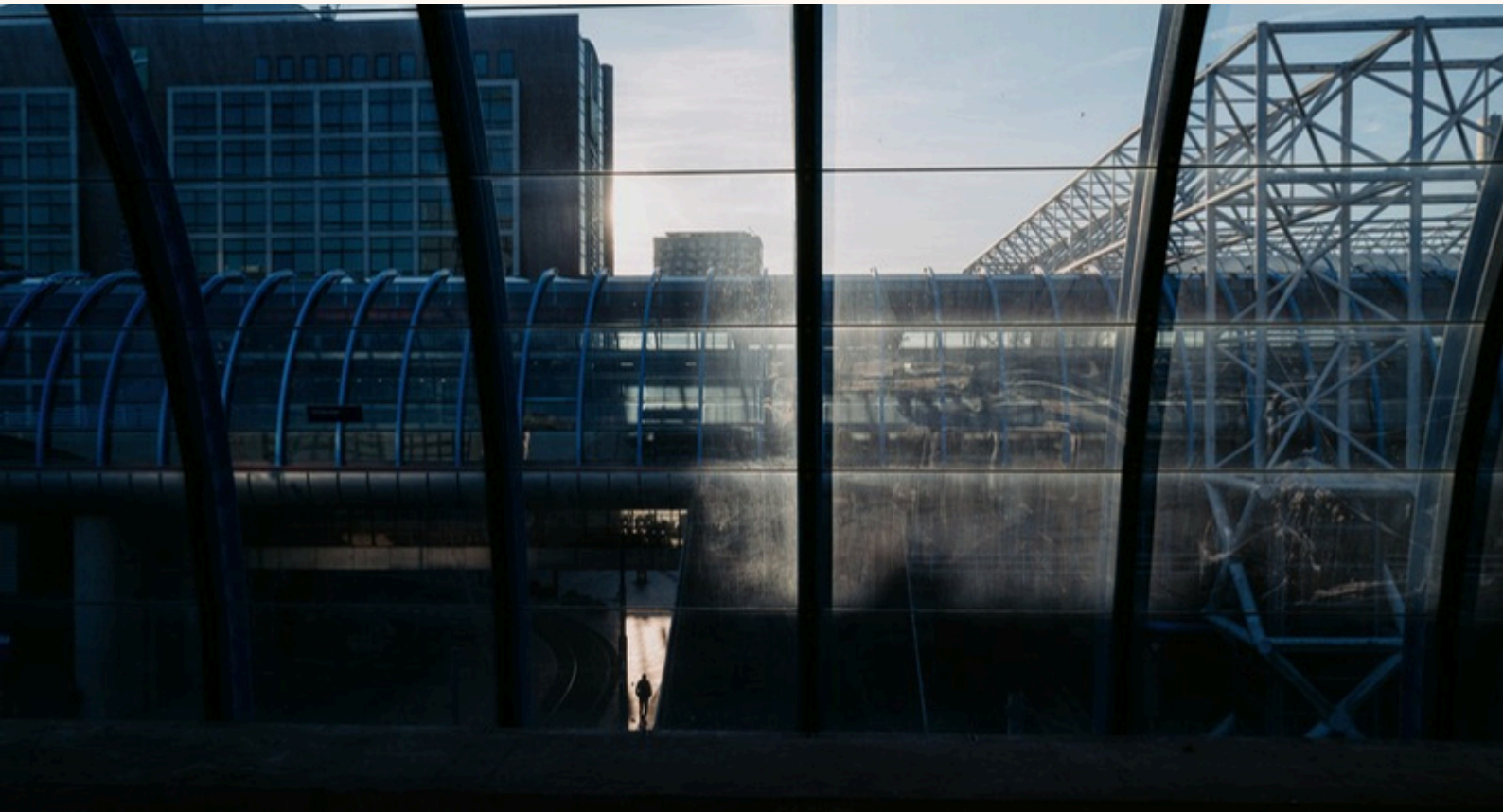
security throughout the entire support period or expected lifespan.

Transparency

users gain insight into cybersecurity characteristics and support period.

Incident response

actively exploited vulnerabilities and serious incidents are reported to supervisory authorities and (affected) users.



Why does the CRA exist, and when does it take effect?

Central premise: anything connected to the internet (or a comparable digital network) is at risk of being hacked. The CRA requires organisations to take appropriate measures: prevent vulnerabilities, monitor whether digital intruders (criminals or even hostile state actors) have gained access, and act swiftly if they have. The more important or sensitive the product and the greater the potential damage, the more stringent the measures must be.

Date	What takes effect?
11 June 2026	Notification of notified body (Chapter IV)
11 September 2026	Reporting obligation for vulnerabilities and incidents (Art. 14)
11 December 2027	Full application (conformity assessment, CE marking, technical documentation)

Please note: the reporting obligation takes effect **15 months earlier** than most other obligations, and also applies to products already placed on the market. Therefore, determine before 11 September 2026 whether your organisation falls under the CRA and the reporting obligation.

What does this mean in practice?

Product categories

The CRA distinguishes product categories with requirements for security and for demonstrating conformity, appropriate to the risks: **default, important class I or II, and critical.** The category determines the conformity route (internal control, external party or notified body, or certificate with at least "substantial" assurance level). For critical products (Annex IV), mandatory European cybersecurity certification may be prescribed via a delegated act.

Five roles under the CRA

- **Manufacturer:** develops (or commissions the development of) products placed on the market under its own name or trademark, or substantially modifies products.
- **Authorised representative:** party representing a manufacturer established outside the EU.
- **Importer:** places products from outside the EU on the market.
- **Distributor:** makes products available without affecting their properties.
- **Open-source software steward:** maintains open-source software without being a manufacturer.

Reporting obligation: 3-phase model

Manufacturers must report actively exploited vulnerabilities and serious incidents to the competent CSIRT and to ENISA, via the Single Reporting Platform (SRP) that ENISA is establishing (Art. 16).

Phase	Deadline	Content
Early warning	Within 24 hours of becoming aware	Indication of affected Member States. For incidents: at minimum, whether it was presumably caused by unlawful or malicious acts.
Vulnerability or incident notification	Within 72 hours of becoming aware	General information about the product, nature of exploitation or incident, initial assessment, risk mitigation measures taken, corrective measures for users.
Final report	Vulnerability: within 14 days after corrective measure is available. Incident: within 1 month after incident notification.	Description, severity, consequences, cause, malicious actor, security update or details of corrective measures.

Informing users

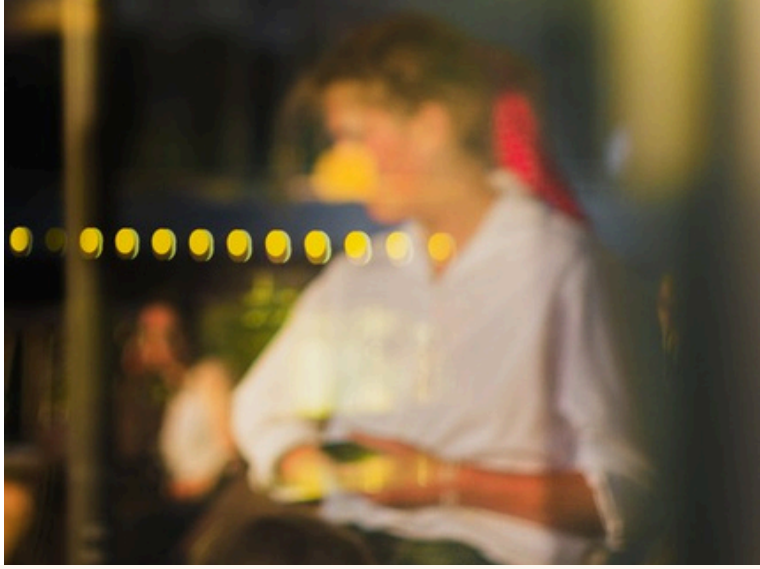
in addition to reporting to CSIRT/ENISA, the manufacturer must inform affected users (and, where appropriate, all users) of the vulnerability or incident and of risk mitigation measures, preferably in a structured, machine-readable format such as a directly executable security update (Art. 14(8)). Care must be taken to prevent the information from being misused by (other) malicious actors.

Voluntary reporting

manufacturers and other natural or legal persons may also voluntarily report vulnerabilities, cyber threats and incidents to CSIRTs. If someone other than the manufacturer reports, the CSIRT informs the manufacturer.

Notified bodies (from 11 June 2026)

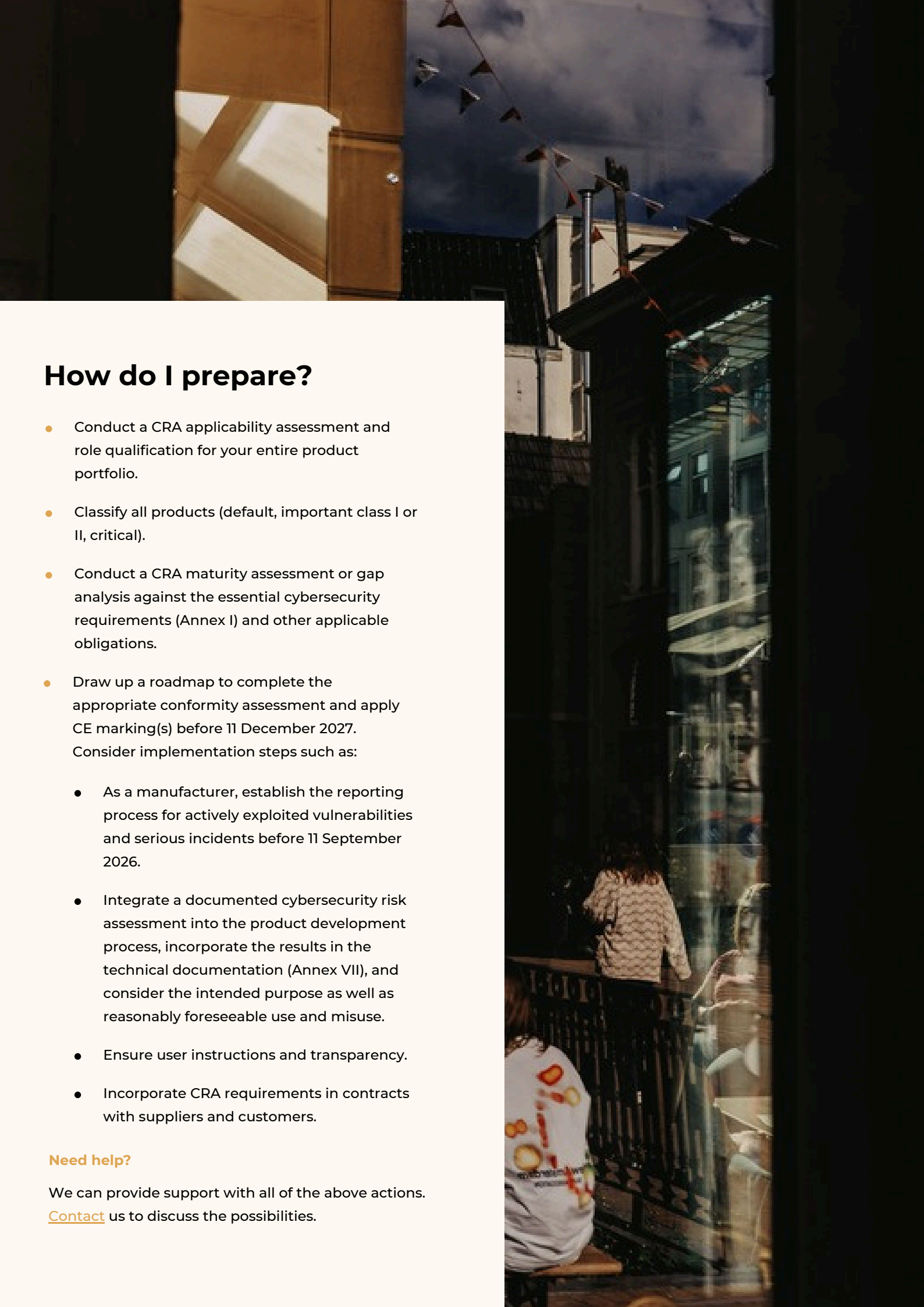
Pursuant to Art. 71(2), the provisions on notification of conformity assessment bodies (Chapter IV, Art. 35–51, referred to as "notified bodies") apply from 11 June 2026. This is particularly relevant for important and critical products: manufacturers must approach a notified body in good time for conformity assessment and CE marking.



Sanctions

Infringement	Maximum fine
Breach of essential requirements (Annex I) or Art. 13/14	€15 million or 2.5% of global annual turnover
Breach of other obligations (including Art. 18–23, 28, 30–33, 39, 41, 47, 49, 53)	€10 million or 2% of global annual turnover
Incorrect or misleading information to notified bodies or market surveillance	€5 million or 1% of global annual turnover

Micro and small enterprises do not receive a fine for exceeding the 24-hour deadline (Art. 64(10).

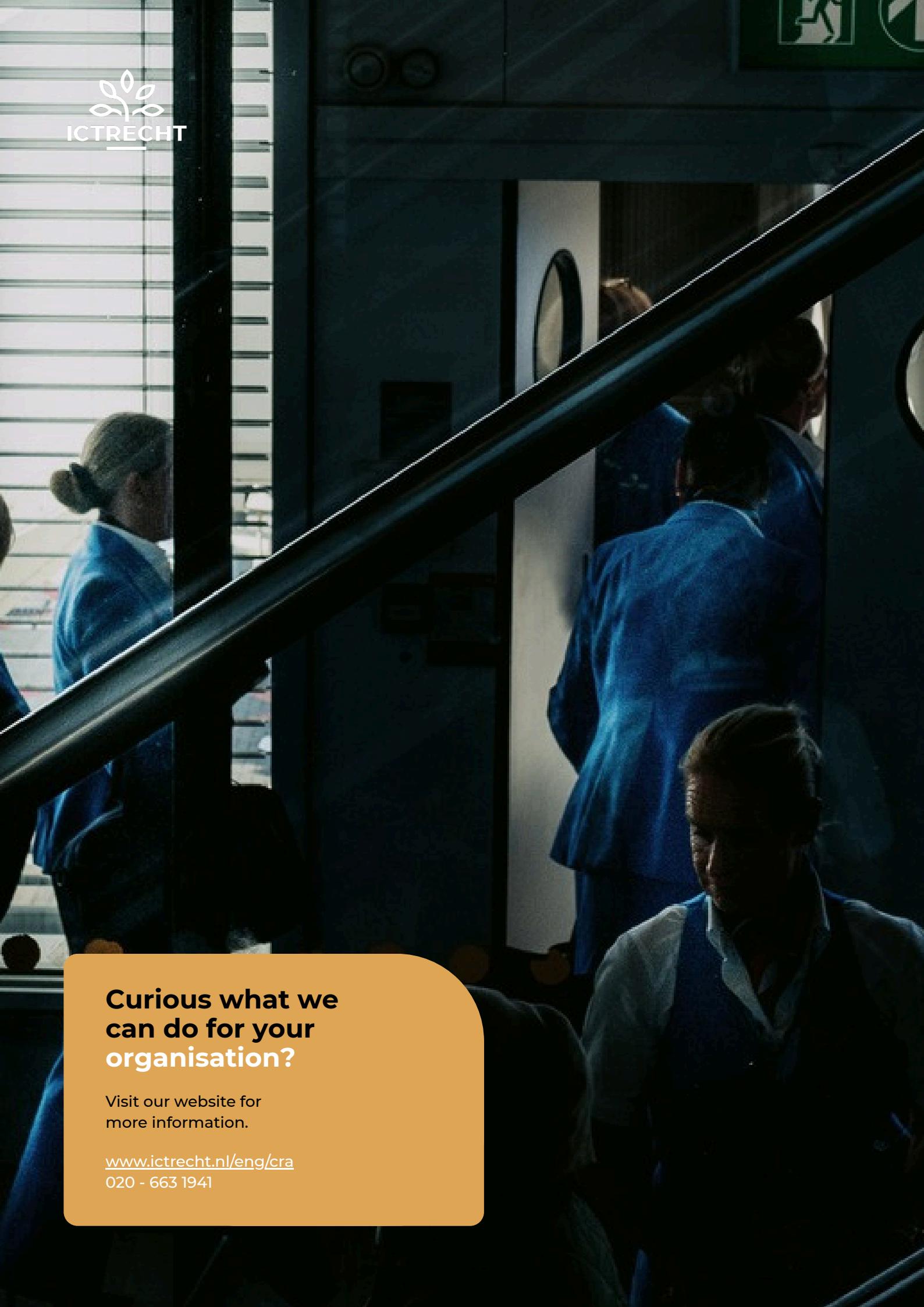


How do I prepare?

- Conduct a CRA applicability assessment and role qualification for your entire product portfolio.
- Classify all products (default, important class I or II, critical).
- Conduct a CRA maturity assessment or gap analysis against the essential cybersecurity requirements (Annex I) and other applicable obligations.
- Draw up a roadmap to complete the appropriate conformity assessment and apply CE marking(s) before 11 December 2027. Consider implementation steps such as:
    - As a manufacturer, establish the reporting process for actively exploited vulnerabilities and serious incidents before 11 September 2026.
    - Integrate a documented cybersecurity risk assessment into the product development process, incorporate the results in the technical documentation (Annex VII), and consider the intended purpose as well as reasonably foreseeable use and misuse.
    - Ensure user instructions and transparency.
    - Incorporate CRA requirements in contracts with suppliers and customers.

Need help?

We can provide support with all of the above actions. Contact us to discuss the possibilities.



ICTRECHT

Curious what we can do for your organisation?

Visit our website for more information.

www.ictrecht.nl/eng/cra
020 - 663 1941