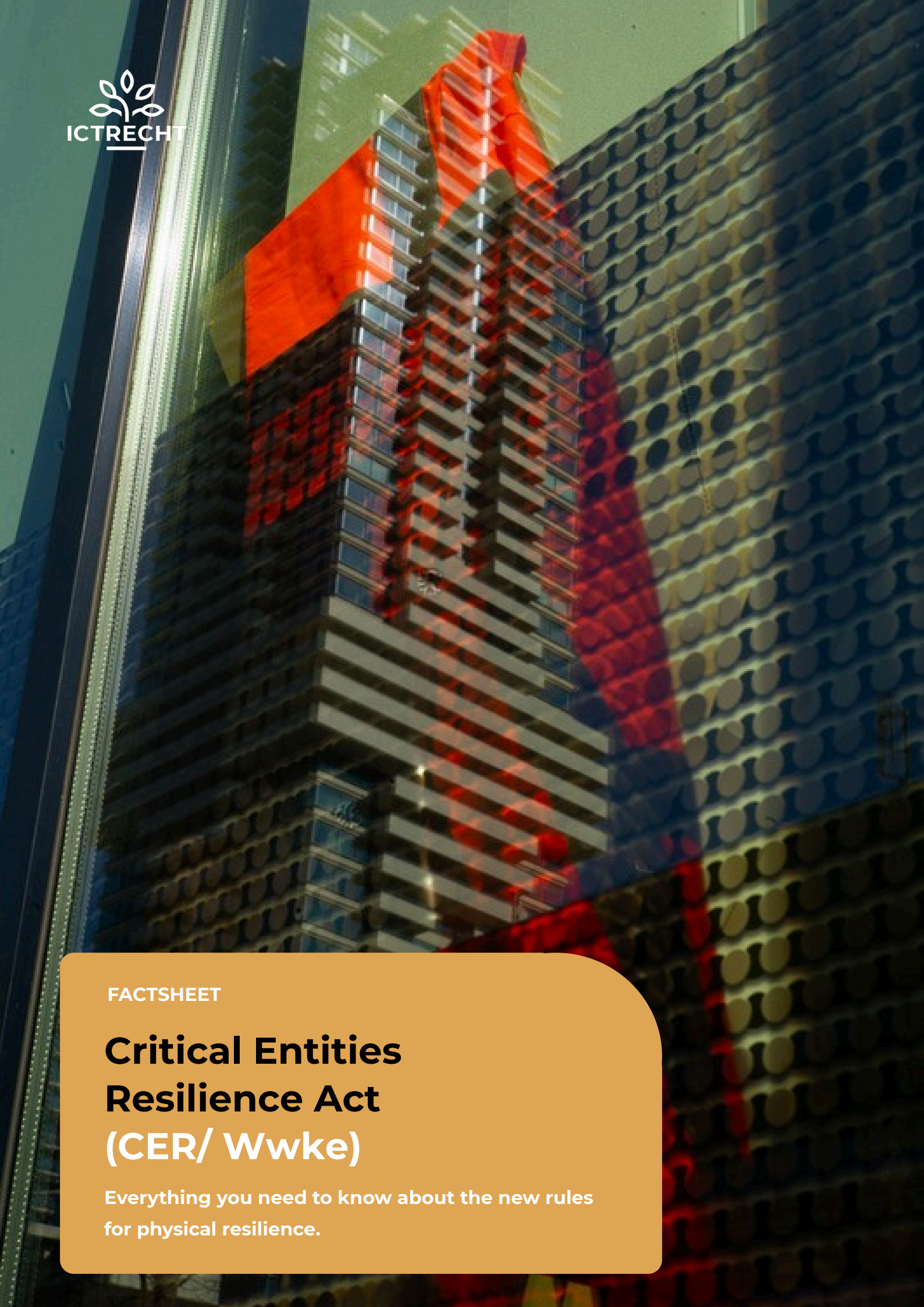


ICTRECHT

FACTSHEET

Critical Entities Resilience Act (CER/ Wwke)

Everything you need to know about the new rules for physical resilience.

Scope

What is the Critical Entities Resilience Act?

The Wwke is the Dutch implementation of the European CER Directive (Directive (EU) 2022/2557 on the resilience of critical entities). The Act aims to maintain vital societal functions and economic activities by strengthening the resilience of critical entities and their ability to provide essential services.

The Wwke is the physical counterpart to the Cybersecurity Act (Cbw/NIS2): while the Cbw focuses on digital resilience, the Wwke addresses all other risks and threats, such as natural disasters, sabotage, terrorism and hybrid threats. The Wwke expressly does not apply to matters covered by the Cybersecurity Act.

Objectives

The Act is built on the following pillars:

Risk assessment

Identifying and assessing relevant (non-cyber) risks to essential services.

Resilience measures

Taking appropriate technical, security and organisational measures.

Incident notification

Reporting significant disruptions to essential services.

Cooperation and information sharing

Sharing information and best practices between competent authorities and critical entities, including cross-border.

Sectors (Annex to the Act):

The Wwke applies to entities in the sectors listed in the Annex to the Act:

Wwke sectors (Annex to the Act)

- Energy (electricity, district heating/cooling, oil, gas, hydrogen)
- Transport
- Banking
- Financial market infrastructure
- Healthcare
- Drinking water
- Wastewater
- Digital infrastructure
- Public administration
- Space
- Production, processing and distribution of food

Additional sectors may be designated by governmental decree under Article 7(1).

Who does it apply to?

The Wwke applies to critical entities: entities designated as such by the competent authority because they provide one or more essential services within one of the sectors listed in the Annex to the Act.

Under the CER Directive on which the Wwke is based, an entity is designated as a critical entity when:

1. It provides an essential service in a sector listed in the Annex;
2. It operates on Dutch territory; and
3. An incident would have a significant disruptive effect on the provision of one or more essential services in the Netherlands or other Member States.

Exemptions
The Act does not apply to:

- The Ministry of Defence;
- The intelligence and security services (Wiv 2017);
- The Public Prosecution Service;
- The police;
- The safety regions (Article 9, Safety Regions Act);
- Other government bodies designated by governmental decree that primarily carry out activities in the area of national security, public security, defence or law enforcement (including the investigation and prosecution of criminal offences).

Matters covered by the Cybersecurity Act also fall outside the scope of the Wwke.

Note (overlap with Cbw/NIS2):
If you are designated as a critical entity under the Wwke, the Cbw automatically applies. This is the case even if you do not meet the Cbw's application criteria.

Critical entity: designation and list

Unlike the Cbw (where organisations assess themselves whether they fall under the Act), the Wwke operates through a **designation system by the competent authority.**

Who decides?

The competent authority designates critical entities.

Basis

Provision of an essential service + significant disruptive effect in case of an incident.

Lijst

The competent authority draws up and updates a list of critical entities **at least every four years,** or more frequently if necessary.

Role of the competent authority

The competent authority (designated under Article 8) actively supports critical entities. Cooperation includes at minimum the exchange of information and best practices, and may (following consultation with the Minister) also include:

A) developing guidelines and methodologies;

B) providing assistance in crisis or emergency situations;

C) helping to organise exercises to test resilience;

D) providing advice to critical entity staff;

E) providing training to critical entity staff.

Single point of contact

The Minister of Justice and Security is the single point of contact and has the following responsibilities:

- Liaison function with the European Commission;
- Cross-border cooperation with single points of contact of other EU Member States and with the Critical Entities Resilience Group (Article 19 CER Directive);
- Cooperation with competent authorities of third countries;
- Ensuring cross-sectoral and effective cooperation between competent authorities within the Netherlands.

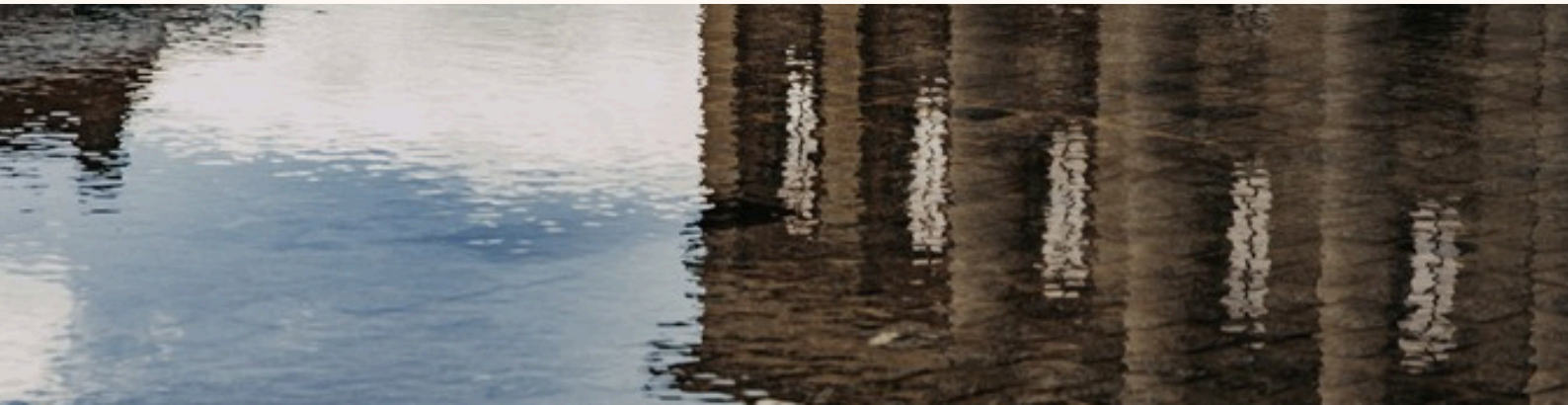
Obligations

National strategy

The Minister of Justice and Security (in agreement with the relevant ministers) establishes a strategy on the resilience of critical entities. This strategy includes at minimum:

Element	Explanation
Objectives and priorities	Taking into account cross-border and cross-sectoral dependencies.
Governance framework	Tasks and responsibilities of authorities, critical entities and other parties.
Measures	Including a description of the risk assessments (Article 9).
Identification process	How critical entities are identified.
Support process	Including public-private cooperation.
Authorities and stakeholders	List of key parties involved.
Coordination framework	Coordination with the competent authority under the Cbw (Art. 15 Cybersecurity Act) for information sharing on both cyber and non-cyber risks.
SME support	Measures to facilitate compliance for small and medium-sized critical entities.

The strategy is updated **at least every four years,** following consultation with relevant parties.



Obligations for critical entities (Articles 14, 15, 17)

Critical entities must (as further detailed in the Act and underlying regulations):

Obligation	Explanation
Risk assessment	Carry out a risk assessment of all relevant (non-cyber) risks that could disrupt essential services.
Resilience measures	Take appropriate and proportionate technical, security and organisational measures to prevent, protect, respond, withstand, mitigate, recover and adapt.
Incident notification	Report incidents that significantly disrupt or could significantly disrupt the provision of essential services.
Background checks	Carry out background checks for certain positions (where provided for in further regulations).
Contact person	Designate a liaison officer to the competent authority.

Implementing and delegated acts

Additional rules may be laid down by or pursuant to governmental decree to implement the implementing acts, delegated acts and guidelines adopted under the CER Directive. Keep a close eye on these underlying regulations.

Incident notification obligation

Critical entities report significant incidents to the competent authority. An incident is significant when it significantly disrupts or could significantly disrupt the provision of essential services. The specific thresholds and notification deadlines will be further specified by governmental decree or ministerial regulation.

Note:
If an incident also constitutes a cyber incident, there may also be a notification obligation under the Cybersecurity Act. In the case of a data breach, the notification obligation to the Dutch Data Protection Authority (AP) applies as well.

Supervision, sanctions and timeline

Supervision

The competent authority (designated under Article 8 Wwke) supervises compliance with the obligations by critical entities. It works closely with the competent authority under the Cybersecurity Act to share information on both cyber and non-cyber risks, threats and incidents.

Sanctions regime

In case of non-compliance, the competent authority may deploy the following instruments, among others:

Sanction	Explanation
Warning	For less serious violations
Binding instruction	Mandatory instructions to achieve compliance
Order subject to periodic penalty payment	Penalty payment until compliance is achieved
Administrative fine	Financial sanction (amount to be determined by or pursuant to the Act)

The specific maximum fine amounts under the Wwke differ from those under the Cbw and should be verified in the specific fine provisions of the Act and underlying regulations.

Relationship with the Cybersecurity Act

Both Acts complement each other:

Aspect	Wwke
Focus	Physical/non-cyber resilience
EU-basis	CER Directive (2022/2557)
Designation	By competent authority
Coordination	Mandatory coordination framework between both competent authorities

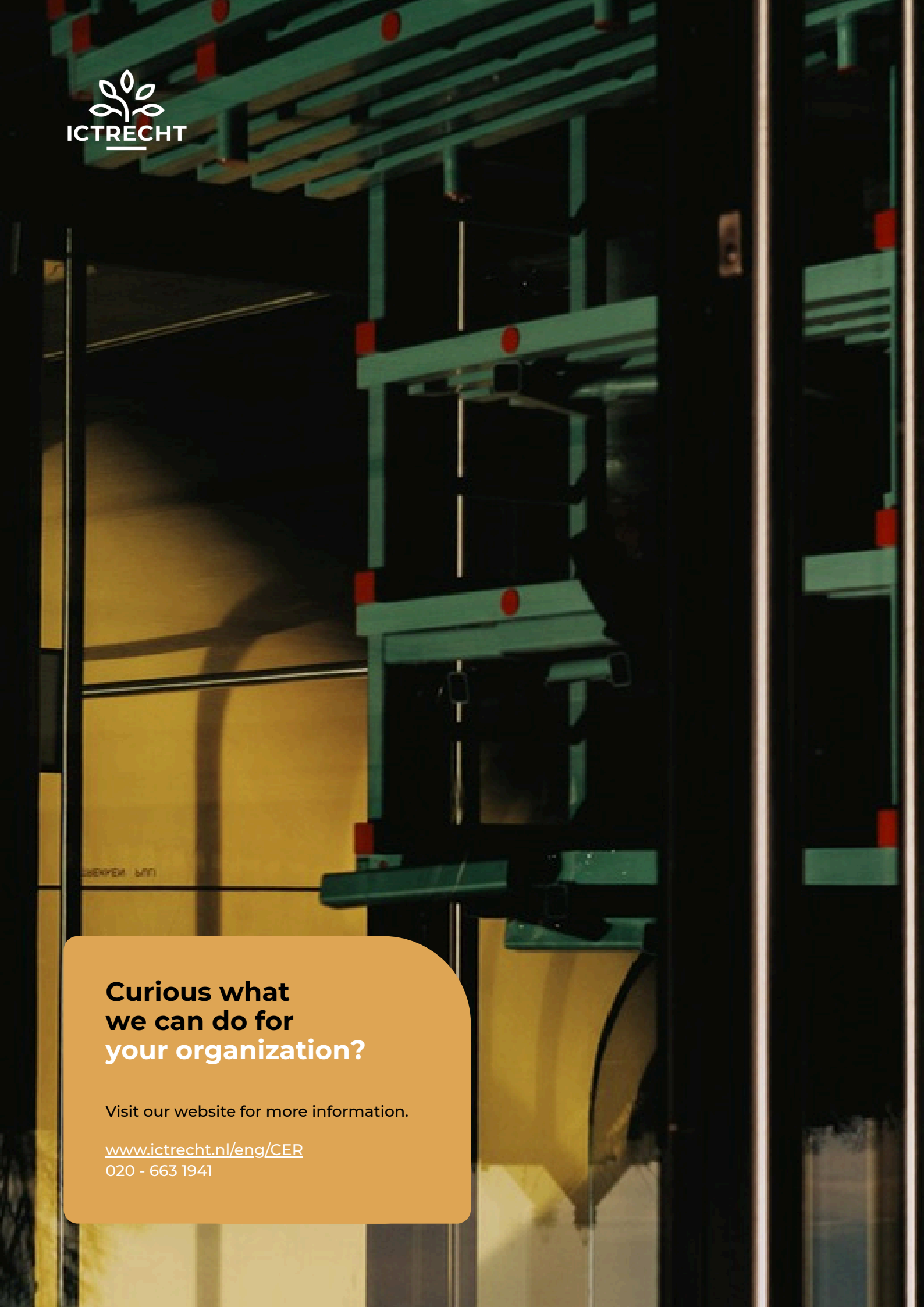
Timeline:

Datum	Gebeurtenis
14 December 2022	CER Directive (EU) 2022/2557 adopted
17 October 2024	Deadline for CER Directive implementation (the Netherlands is behind schedule)
June 2025	Bill submitted to the House of Representatives
15 April 2026	House of Representatives approves the Critical Entities Resilience Act
7 July 2026	Senate approves the Critical Entities Resilience Act
15 August 2026	Critical Entities Resilience Act enters into force

Recommended actions if you are designated:

1. Conduct a GAP analysis on physical and organisational resilience (in addition to existing cyber analyses);
2. Draw up an all-hazards risk assessment and implementation plan;
3. Set up coordination between your Wwke and Cbw compliance efforts (governance, notification procedures, contact persons);
4. Prepare registration, notification and background check procedures.

These are actions ICTRecht can help you with.



ICTRECHT

Curious what we can do for your organization?

Visit our website for more information.

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