Critical Entities Resilience Directive

Compliance insights on ensuring resilience for critical infrastructure

May 2025

In this Whitepaper, we provide an overview of the Critical Entities Resilience (CER) Directive, focusing on what organisations within the European Union (EU) need to know to prepare for compliance.

Often overlooked as the sister Directive to NIS2, CER aims to strengthen the EU's resilience by addressing physical threats to critical infrastructure, where NIS2 addresses the digital threats. As such, CER should be a priority for all critical entities in the EU alongside NIS2. In this paper, we share our understanding of the CER Directive, highlight key requirements and scoping criteria, and offer recent insights and developments based on the work we do for our clients.

Understanding the Directive

The EU is taking decisive steps to strengthen the resilience of critical and digital infrastructure against both offline and online threats. Recent crises – such as the COVID-19 pandemic, the war in Ukraine, and climate-related disasters – have underscored the urgent need for greater collective preparedness.

However, increasing interconnectivity, complex supply chains, fragmented sector-specific regulations, and inconsistent definitions of 'critical' infrastructure have all posed significant challenges to effective resilience planning and implementation across the EU.

To address these challenges, the EU introduced two sister Directives in January 2023: the CER Directive (EU Directive 2022/2557) and the NIS2 Directive (EU Directive 2022/2555). These Directives aim to strengthen the EU's resilience to growing physical and digital threats by harmonising rules and definitions around resilience measures.

While NIS2 addresses cyber threats to network and information systems, CER focuses on strengthening the physical security and operational resilience of essential services across 11 key sectors, including energy, transport, health, and banking. It adopts an all-hazards approach, covering a wide spectrum of risks from natural disasters and terrorist attacks to sabotage and insider threats.

The regulatory timeline

Member States were required to transpose the CER Directive into national law by **17 October 2024**. By **17 January 2026**, they must have adopted a national strategy to strengthen the resilience of critical entities and completed a risk assessment to identify those entities. These critical entities must be identified latest **17 July 2026**, and once an organisation is designated as a critical entity, it will have ten months to comply with the Directive's requirements. This brings the latest compliance deadline for critical entities to **May 2027**.

Timeline

- **17 October 2024** | Deadline for transposing the Directive into national legislation by Member States
- **17 January 2026** | Deadline for Member States to adopt a national strategy for enhancing the resilience of critical entities, and carry out a risk assessment
- **17 July 2026** | Deadline for Member States to identify critical entities
- **Within one month of identification** | Member States shall inform critical entities of their status
- **Within nine months of receiving notification** | Critical entities must carry out a risk assessment
- **Within 10 months of receiving the notification** | CER requirements apply to critical entities

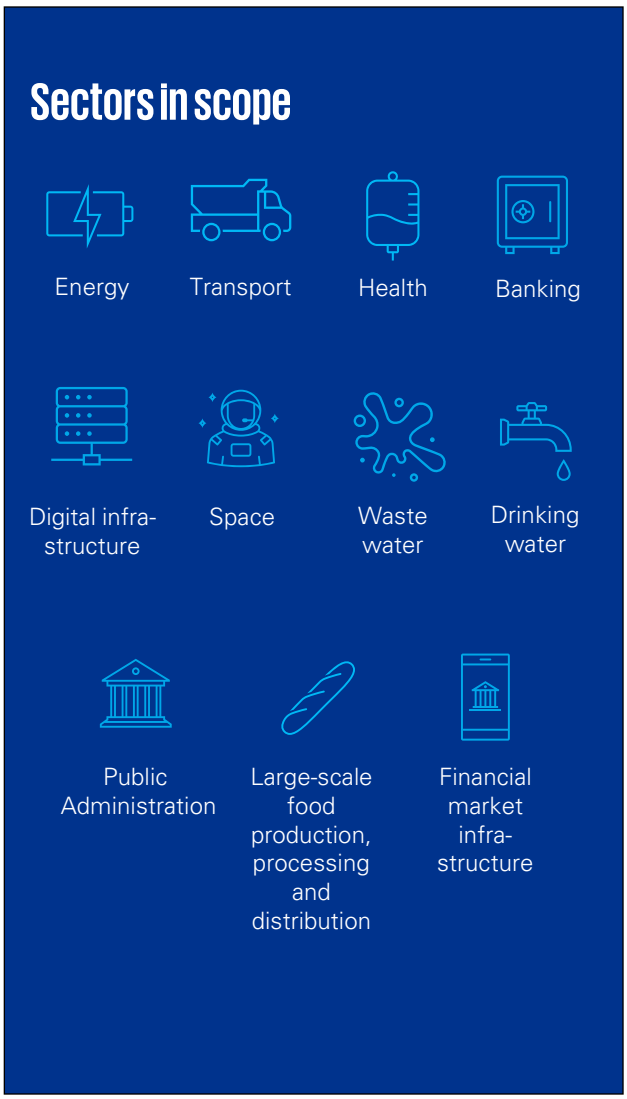
Member State transposition status

The majority of Member States did not meet the October 17 deadline to transpose the CER Directive into national law. As a result, **the European Commission issued formal notice on 28 November 2024**, giving the remaining countries just two months to communicate their transposition measures and complete the transposition process.

Member States are now at varying stages of implementation. For example, the Netherlands missed the October deadline but has since published a draft law that was under public consultation until March 30, 2025, with guidance published from the Dutch Advisory Body (*Raad van State*) on coordination and oversight once the regulation is in place. The CER Directive is expected to come into effect in the Netherlands as a regulation in Q3 2025, roughly a year after the deadline.

Ireland is one Member State that successfully transposed CER into law by October 17, 2024, via Statutory Instrument No. 559 of 2024, titled *the European Union (Resilience of Critical Entities) Regulations 2024*. Further insights into the regulation's requirements can be found on page 4.

Sectors in scope



What are the key requirements critical entities should know about?

Article 12

Critical Entity Risk assessment

The deadline for Member States to identify critical entities is July 17, 2026. Once designated, critical entities have nine months to conduct a risk assessment in accordance with Article 12 of the CER Directive. This sets the latest possible deadline for completing the risk assessment continues April 17, 2027, one month before the full compliance obligations become applicable, which is 17 May 2027 at the latest.

This risk assessment must cover all relevant threats that could disrupt the delivery of essential services, accounting for all relevant natural and man-made risks, including cross-sectoral or cross-border risks, accidents, natural disasters, public health emergencies, and hybrid threats. It must then be updated at least every 4 years, or sooner if needed.

The assessment must also consider dependencies and interdependencies across sectors in scope of CER, with a particular focus on supply chain vulnerabilities within critical infrastructure. This requirement ensures that critical entities stay aware of and prepared for potential disruptions that could impact service continuity.

Reducing the compliance burden

To reduce the burden on critical entities, the CER Directive permits the use of alternative, relevant risk assessments. If an entity has already conducted assessments or prepared documentation under other legal frameworks that align with CER requirements, these can be used to meet Article 12, subject to approval by the relevant competent authority.

Article 13

Resilience measures

Articles 13-16 of the CER Directive become applicable 10 months after an organisation is designated as a critical entity, with the latest possible deadline falling in May 2027. Based on the Member State Risk Assessment (used to identify critical entities) and the Critical Entity Risk Assessment (used to identify specific risks to their essential services), designated entities are required to implement appropriate and proportionate technical, security, and organisational measures to ensure their resilience. These measures include:

- Prevention of incidents, considering disaster risk reduction and climate adaptation measures;
- Response to, resisting, and mitigating the consequences of incidents, considering the implementation of risk and crisis management procedures and protocols and alert routines;
- Incident recovery, considering business continuity measures and identification of alternative supply chains;
- Physical protection of premises and critical infrastructure, considering e.g., barriers, perimeter monitoring tools, access controls;
- Employee security management, considering measures such as access rights, setting up background check procedures (in accordance with Article 14), training and qualifications;
- Raising awareness on the listed resilience measures, considering training courses;
- Have in place and apply a resilience plan (or equivalent document) which describes the measures taken.

Each critical entity must also designate a liaison officer or equivalent as the point of contact with the competent authorities, ensuring effective communication and coordination between the entity and the competent authorities.

Article 15

Incident notification

Critical entities must notify the competent authority in a timely manner of incidents that significantly disrupt or have the potential to significantly disrupt the provision of their essential services.

To determine the significance of an incident, the following should be considered:

- Number and proportion of users affected
- Duration of disruption
- Geographical areas affected

The critical entities are required to notify the competent authority:

1. 24 hours after becoming aware of the incident (initial notification);
2. 1-month after the incident (detailed incident report),

Example scenario	Incident reportable?
A storm knocks out power to a water treatment plant, causing a disruption in water supply	**Likely yes** | A physical incident causing a disruption to critical infrastructure.
Localised 2-hour power outage with no critical impact	**Likely no** | Localised and not significant disruption to provision of essential services.
Large-scale IT service outage affecting emergency services	**Likely yes under CER and NIS2** | Significantly disrupting the provision of essential services (CER) and operational impact on network and information systems (NIS2).

Notifications must include all relevant information needed for the competent authority to understand the nature, cause, and potential consequences of an incident. This requirement ensures timely awareness, enabling authorities to respond effectively and mitigate the impact.

Article 14

Background checks

Member States will define the conditions for critical entities to request proportionate and necessary background checks on personnel in sensitive roles or with access to critical infrastructure, ensuring they do not pose a security risk.

Article 9 & 10

Cooperation and information sharing

Critical entities must work with authorities and other relevant entities to enhance resilience by sharing information on risks, incidents, and best practices, and participating in exercises and training. This cooperation fosters a coordinated approach to resilience across sectors and Member States.

Scoping requirements

The CER Directive scopes entities into two groups: 'critical entities' and 'critical entities of particular European significance'. The primary distinction is based on the geographic reach of the services provided.

Critical entities

By July 2026, each Member State must have identified the critical entities for each sector and subsector in-scope of CER. This identification will be based on both the Member State Risk Assessment and the Member State Strategy for enhancing the resilience of critical entities, both of which must be completed by 17 January 2026 at the latest.

The identified entities are those who provide essential services that are crucial for maintaining vital societal functions, economic activities, public health and safety, or the environment.

A critical entity will be derived from three criteria:

1. The entity provides one or more essential services;
2. The entity operates, and its critical infrastructure is located, on the territory of that Member State;
3. An incident would have significant disruptive effects, on the provision by the entity of one or more essential services or on the provision of other essential services in the sectors that depend on that or those essential services.

Critical entities of 'particular European significance'

Once identified as a critical entity, the organisation must inform the relevant competent authorities if it provides essential services in six or more Member States. If so, it will be designated as a 'critical entity of particular European significance'. The competent authority will then notify the Commission, which will consult with the entity and the relevant Member States to confirm this status.

In addition to meeting the same resilience requirements as critical entities, these entities are also subject to additional advisory missions from the Commission to assess compliance, with support provided if necessary. They should also collaborate closely with national and EU authorities to ensure coordinated resilience efforts.

Penalties

Below is the CER Directive's specification for penalties upon non-compliance under CER. Additionally, the Irish transposition gives additional insight into how Member States could interpret CER's penalty requirements.

CER Directive

"**Member States shall lay down the rules on penalties** applicable to infringements of the national measures adopted pursuant to this Directive and **shall take all measures necessary** to ensure that they are implemented. The penalties provided for shall be **effective, proportionate and dissuasive**." – Article 22 of CER Directive

Ireland

Ireland has specified a **tiered penalty system** that distinguishes between individuals and non-individuals.

- Non-individuals (e.g., entities) – maximum €500,000;
- Individuals – maximum €50,000.

This emphasis on greater liability for non-individuals reinforces **corporate responsibility** for resilience and security requirements.

Recent insights into CER

As Member States progress with transposing CER and organisations begin preparing for compliance, more context and insights are emerging. This section highlights key developments, including:

Understanding CER's relationship to other regulations is essential for developing a streamlined and unified compliance strategy.

Emerging scoping dilemmas highlight the importance of early clarity on whether an entity falls within scope.

Ireland's early transposition of CER offers valuable insights into how the Directive is being interpreted and applied in practice, serving as a useful reference point for organisations preparing for compliance.

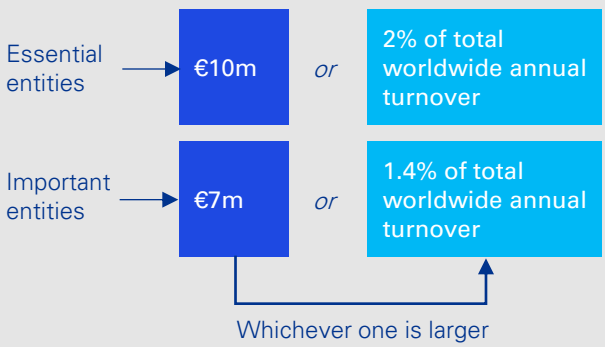
Relationship to other regulation

CER does not exist in a vacuum. The CER Directive is closely aligned with NIS2, with both aimed at strengthening resilience against physical and digital threats across the EU. CER is also aligned with the Digital Operational Resilience Act (DORA), which focuses specifically on enhancing the digital resilience of the financial sector by safeguarding information and communication technology systems against major disruptions.

To avoid regulatory overlap, CER excludes cybersecurity matters already addressed by NIS2 and does not apply to the digital infrastructure or financial sectors, which are regulated under NIS2, DORA, and other sector-specific resilience regulations. These Directives and regulations are intended to be implemented in a coordinated manner to ensure consistency and avoid duplication across compliance requirements.

Importantly, under the NIS2 Directive it states that all critical entities under CER are automatically deemed 'essential' under NIS2. Therefore, they are additionally subject to the most stringent requirements of the NIS2 Directive, as well as its heavy penalties.

NIS2 penalties



Organisations should keep these relationships in mind as they are critical to avoiding duplication of effort and ensuring a unified compliance strategy.

Emerging scoping dilemmas

While CER and NIS2 cover similar sectors, there are key differences in how entities are classified. Under NIS2, the food sector is listed in Annex II, typically designating entities as 'important' rather than 'essential'. In contrast, CER identifies large-scale food production, processing, and distribution as critical.

As noted, entities deemed critical under CER are automatically classified as 'essential' under NIS2, subjecting them to stricter cybersecurity oversight. These differing scopes and classifications create challenges, especially for organisations operating in multiple EU countries. Navigating national variations and overlapping requirements demands a unified compliance strategy that addresses both physical and cyber resilience.

Insights from the Irish transposition of CER

Ireland's CER regulation came into effect on 17 October 2024, in line with the EU deadline. As one of the first fully enacted and accessible implementations, it provides a clear reference for how core CER obligations are applied in practice.

National Risk Assessment

The National Risk Assessment will be conducted every three years in Ireland by the Office of Emergency Planning.

Requirements for Critical Entities

The Irish transposition elaborates in more detail on some of the requirements for critical entities set out by the CER Directive. For example:

Resilience Plans should include:

- Identification of incident scenarios and appropriate prevention measures;
- Precautions for the design, construction, operation, and maintenance of installation, storage facility, equipment, and infrastructure;
- Internal and external emergency plans;
- Requirements for reviewing and updating plans.

Incident notification should include:

- Incident notification (24 hours): details on the essential services affected, the services that may be impacted, and whether an incident might have significant impact on critical entities and essential services in other Member States;
- Incident report (1 month): details on the circumstances of the incident, the data available for assessing the effect, the immediate mitigation measures taken, medium- and long-term mitigation measures, and future prevention steps.

Competent Authorities

- Ireland designated competent authorities for all the 11 sectors in scope, with some sectors having more than one competent authority responsible for different sub-sectors.

National Strategy

- The Office of Emergency Planning in the Department of Defence is Ireland's designated Single Point of Contact. Through collaboration between the competent authorities and with the coordination of the Government Task Force on Emergency Planning, the National Strategy for the Resilience of Critical Entities will be created a delivered by Q1 2026.

Summary

This Whitepaper has provided an overview of the CER Directive, its purpose within the EU regulatory landscape, transposition timelines, key requirements for critical entities, and scoping criteria. It also highlights recent developments to help organisations better understand how to prepare for compliance. To confront the compliance challenge this brings, it is essential to bring these topics to the forefront of the organisation's agenda. Management should be actively engaged and help to align all affected departments.

How KPMG can help

Like other Directives and regulations, the true complexity of CER lies beneath the surface. Determining whether your organisation falls within scope, interpreting national variations, conducting risk and gap assessments, and aligning with supervisory expectations can quickly become overwhelming, especially given the wave of other regulation organisations are currently facing.

Critical entities must look beyond the headlines to uncover hidden obligations and dependencies, and this is where deep expertise makes the difference.

KPMG helps organisations with an end-to-end compliance program, starting from project management and ranging to full-scale implementation. We offer a trusted partnership, being there alongside our clients every step of the way to meet their individual and tailored needs.

With the requirement that all critical entities under CER automatically fall under NIS2, KPMG provides a unified compliance approach, simultaneously preparing organisations for compliance with both Directives. Based on our expertise from previous engagements, knowledge of regulatory timelines and local requirements, as well as our EMA community, we take a risk-based approach to compliance to prioritise the resilience of your organisation.

To kick-start your organisation's compliance journey, we assist with multi-phase compliance programs (our 4-step approach is detailed on the right). In parallel, we can also carry out a NIS2 assessment to ensure alignment and maximise efficiency across both regulatory frameworks.

By partnering with KPMG, organisations can proactively address both CER and NIS2 requirements, enhancing physical, operational and cyber resilience.

Reach out to our experts below to learn more about our tailored approach.

- Our **scoping assessment** determines the applicability and scope of CER for organisation's operations across the EU.
- We conduct a **gap assessment**, mapping policies, standards, and procedures against CER requirements, then carrying out a **risk assessment** to identify vulnerabilities and prioritize mitigation.
- We transfer the insights gained during the assessments into a clear and **actionable roadmap** to take forward into implementation.
- We create specific, actionable plans in a remediation plan, and execute the plan by **implementing improvement actions**.

Our experts

Ronald Heil
Partner - Cyber & TechLaw
KPMG Advisory N.V.
heil.ronald@kpmg.nl
+31 (0)6 51369785

Anna Herrmann
Consultant - Cyber & TechLaw
KPMG Advisory N.V.
herrmann.anna@kpmg.nl
+31 (0)6 57527609