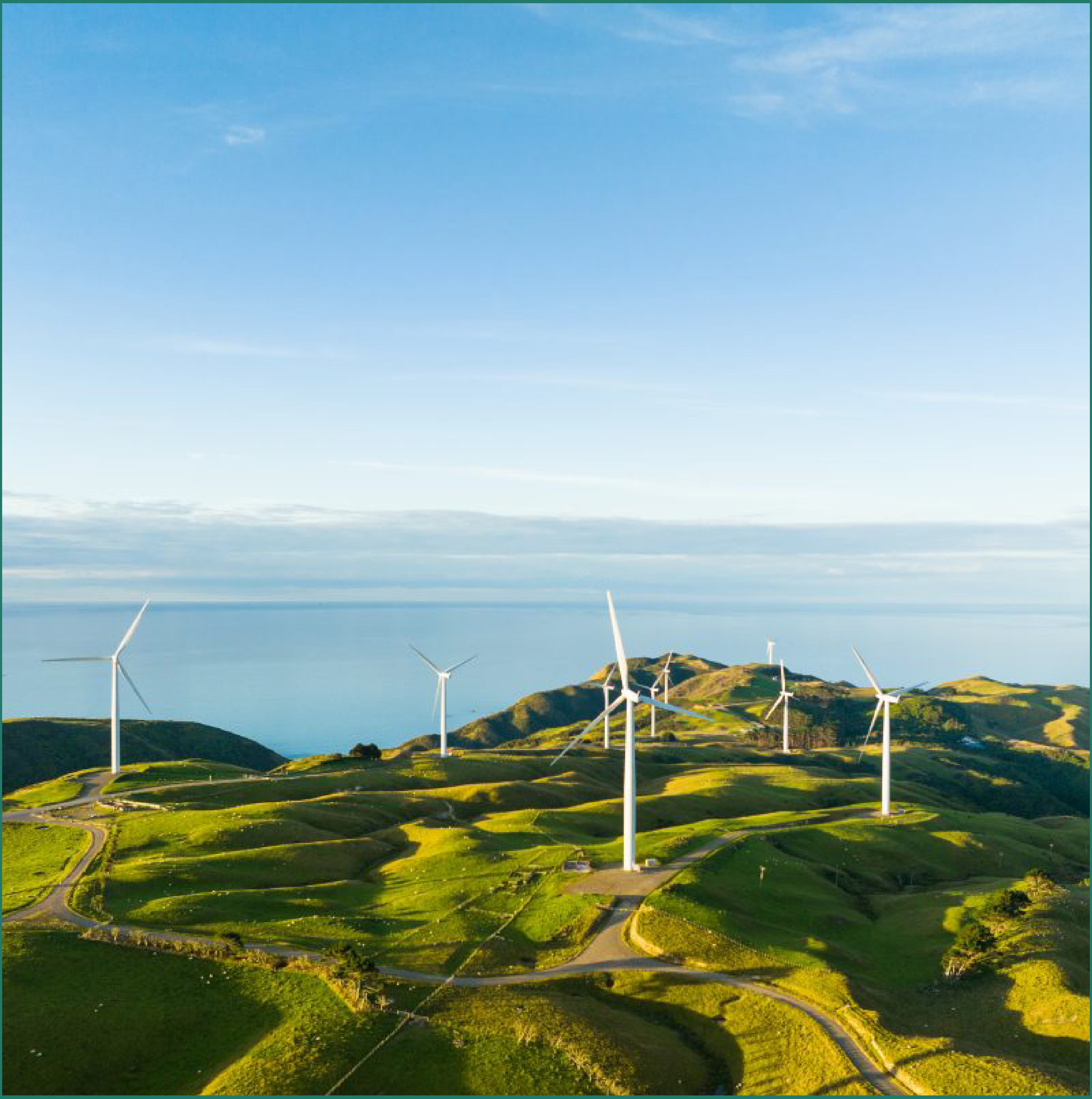


# Understanding the Critical Entities Resilience regime in Ireland

## The Critical Entities Resilience (CER) Directive (Directive (EU) 2022/2557) establishes a harmonised EU framework to strengthen the resilience of organisations that provide essential services.

Unlike sustainability reporting regimes, CER is an all-hazards measure focused on operational resilience. It addresses:

- Natural hazards
- Accidents and public health emergencies
- Terrorism
- Sabotage
- Insider threats
- Hybrid threats

Climate-related risk falls within its scope, but as one hazard category among many rather than the organising principle.

There is increasing overlap between sustainability, risk and resilience capabilities – particularly in areas such as energy, supply chains and critical infrastructure.

### The Irish regulations

In Ireland, the Directive has been transposed through S.I. No. 559 of 2024. Implementation is now progressing through national strategy, risk assessment and entity designation, led by the Department of Defence through the Office of Emergency Planning.

Regulation 2 defines resilience as a critical entity's ability to "prevent, protect against, respond to, resist, mitigate, absorb, accommodate and recover from an incident."

Statutory obligations apply only to designated entities. However, expectations for board-level oversight of resilience are already emerging in governance practice and supervisory expectations.

These expectations are also likely to extend across value chains. Organisations may be asked to provide resilience-related information, assurances and continuity commitments. Some capabilities developed under CSRD (and emerging under CSDDD) – particularly supply chain mapping and risk identification – may be directly transferable.

CER marks a shift from compliance as disclosure to compliance as operational preparedness.

### Organisations in scope

CER applies to organisations designated as critical entities by the relevant competent authority within eleven sectors:

- Energy
- Transport
- Banking
- Financial market infrastructure
- Health
- Drinking water
- Wastewater
- Digital infrastructure
- Public administration
- Space
- Large-scale food production, processing and distribution

An organisation is likely to be designated where it:

- Provides essential services.
- Operates in the State with relevant infrastructure located here.
- Would cause significant disruption if those services were unavailable.

Competent authorities must identify critical entities by 17 July 2026, after which notification letters begin to issue and each designated entity's compliance clock starts. Designation is carried out by competent authorities working with the Department of Defence. Many organisations that may be in scope are unlikely to be aware that assessment is already under way.

## CER requirements for designated entities

Following notification, designated entities must:

- Carry out an entity-level, all-hazards risk assessment.
- Implement technical, security and organisational measures to prevent and manage disruption.
- Notify significant incidents to the competent authority.
- Apply background checks for sensitive roles, where appropriate and permitted.
- Designate a point of contact and cooperate with oversight and inspections.

Initial requirements – particularly risk assessment – arise within months of notification, ahead of the broader implementation window.

For many entities, the most intensive phase is likely to fall in 2027. However, decisions on scope are being made now.

- Risk assessment: within nine months of notification (Regulation 15).
- Resilience plan or equivalent: within ten months of notification (Regulation 16).
- The Regulations apply in full ten months after notification (Regulation 12).
- Incident notification: initial report within 24 hours of awareness, detailed report within one month (Regulation 18).

## Governing CER in Ireland

CER replaces the European Critical Infrastructure (ECI) Directive. This shifts the focus from protecting discrete infrastructure assets to ensuring the continuity of essential services across interconnected systems and dependencies.

Ireland transposed CER through the European Union (Resilience of Critical Entities) Regulations 2024 (S.I. No. 559 of 2024), made by the Minister for Defence and in operation since 17 October 2024.

The Office of Emergency Planning, within the Department of Defence, acts as the national Single Point of Contact, with sector-specific competent authorities responsible for each of the eleven sectors. The National Strategy on the Resilience of Critical Entities 2026–2029, published on 19 March 2026, supports the identification process alongside the updated National Risk Assessment.

The Strategy is a core requirement of the Directive and underpins designation.

## How does CER relate to NIS2?

CER is the physical and all-hazards counterpart to the NIS2 Directive (Directive (EU) 2022/2555), which addresses cyber security. In Ireland, NIS2 is led by the National Cyber Security Centre, now under the Department of Justice, Home Affairs and Migration, while CER is led by the Department of Defence.

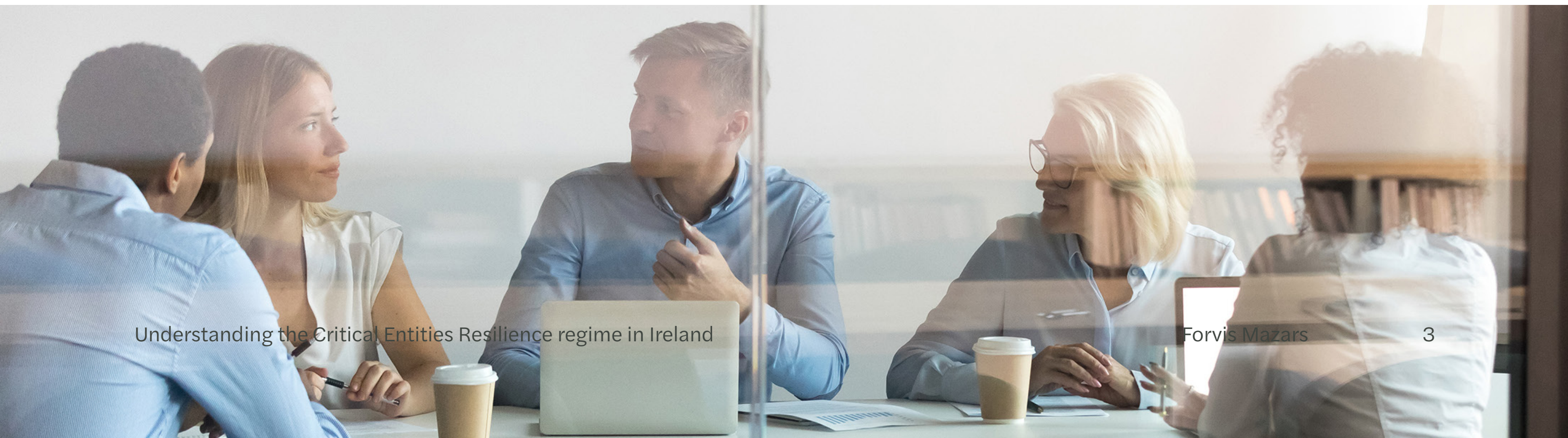
That these responsibilities now sit across Defence, Justice and sectoral regulators rather than in any single department is itself the point: resilience ownership in Ireland is being redistributed, and organisations should expect the same challenge internally.

Some organisations will fall within the scope of both. These organisations should align governance, risk assessment and incident response across both regimes, rather than operating in parallel.

Integrating sustainability, risk and resilience activities can help ensure a more coherent approach.

One important nuance in the Irish Regulations is that critical entities in banking, financial market infrastructure and digital infrastructure that are already identified under NIS2 or DORA are exempt from the core CER obligations (Regulation 3, S.I. No. 559 of 2024), reflecting that their operational resilience is regulated under those regimes.

CER's distinctive requirements therefore bear most heavily on the physical and operational sectors – energy, transport, water, health, food and their supply chains.



## Organisations outside of scope

CER applies directly only to designated entities, but its impact extends further.

Designated entities depend on suppliers to maintain continuity of essential services. As a result, they are likely to seek:

- Resilience assurances
- Dependency information
- Continuity commitments

Organisations outside formal scope – including those already responding to CSRD or NIS2 requirements – may therefore receive CER-related requests from customers.

For these organisations, board oversight of operational resilience remains good governance and an increasingly important commercial consideration.

These resilience-related requests are not constrained by sustainability reporting boundaries, even where similar supply chain data has already been developed for CSRD purposes. While related, sustainability and resilience serve distinct, but increasingly connected roles.

Notably, the Omnibus Directive (Directive (EU) 2026/470) capped what CSRD reporters may demand from smaller value-chain partners – but that cap applies to sustainability reporting only. Resilience-related requests under CER sit outside it entirely: a supplier protected from a CSRD questionnaire can still receive a continuity-assurance request from a designated customer, with no statutory limit on what may be asked.

## Status and next steps in Ireland

The Regulations are in force and the National Strategy has recently been published. The next significant milestone is the identification of critical entities by 17 July 2026, after which designated entities will be notified and the compliance timeline will begin.

Organisations operating in the eleven sectors, and their key suppliers, should now:

- Consider whether they are likely to be designated or sit within a designated value chain.
- Assess their current resilience capabilities.
- Review existing CSRD work, particularly value chain mapping and risk identification.

This work can be adapted to treat identified "hot spots" as hazards requiring resilience measures. The current phase, before formal designation, is critical. Organisations have an opportunity to anticipate exposure rather than react to notification.

At its core, CER is concerned not only with identifying risks, but with ensuring the continuity of essential services under disruption.

# Contact

**Liam McKenna**
Partner, Consulting
Email: lmckenna@mazars.ie

**Johnny Meehan**
Head of Supply Chain Resilience &
Sustainability Consulting
Email: johnny.meehan@mazars.ie

Forvis Mazars in Ireland is a leading international audit, tax, advisory and consulting firm. Operating as a united partnership, Forvis Mazars works as one integrated team, leveraging expertise, scale and cultural understanding to deliver exceptional and tailored services in audit, assurance, tax, consulting, financial advisory, corporate finance and financial outsourcing.