Achieving compliance with the EU CER Directive

Changes ahead for critical entities

19 June 2024

Why should I read this?

The "Directive on the resilience of critical entities" (EU Directive 2022/2557) ("**CER Directive**") has been introduced to enhance the resilience of essential entities and infrastructure across Europe and businesses operating in the EU by providing a more robust framework for securing vital services and infrastructure. This directive will repeal and replace the "directive on European Critical Infrastructures" (ECI Directive, 2008/114/EC). The CER Directive entered into force on 16 January 2023. Critical entities provide essential services in upholding key societal functions, supporting the economy, ensuring public health and safety, and preserving the environment.

Member States are required to identify the critical entities within the sectors outlined in the CER Directive by July 17, 2026. They will utilize a list of essential services to conduct risk assessments, which will then help in pinpointing these critical entities. Upon identification, these entities must implement strategies to bolster their resilience.

The CER Directive aims to strengthen the resilience of both public and private entities operating in critical sectors, ensuring they can withstand and recover from disruptive incidents.

What should I do?

The CER Directive, like other EU directives, sets objectives that all Member States must achieve by incorporating them into their national legislation within a defined timeframe. However, it is up to each country to determine how to meet these goals, which can result in variations in the stringency of national laws, provided they meet the minimum standards set by the directive. Consequently, organisations will need to comply with the specific national laws implementing the CER Directive rather than the directive itself. The CER Directive was adopted by the European Parliament and the Council of the European Union on 14 December 2022 and entered into force in January 2023. Key upcoming dates for organisations to keep in mind include:

- October 2024: Member States are required to transpose the CER Directive into national law.
- January 2026: Member States must adopt a national strategy to enhance the resilience of critical entities.
- July 2026: Member States must identify critical entities and notify them within one month of identification.

- The Directive imposes significant requirements for risk management and resilience. Although critical entities may not be designated until July 2026, they will then have only ten months to demonstrate compliance.

What else do I need to know about the CER Directive?

Key aspects of the CER Directive include:

- Expanded scope: the directive now covers a broader range of sectors, including healthcare, energy, transport, and digital infrastructure.
- Enhanced security measures: the CER Directive includes enhanced security measures aimed at strengthening the resilience of critical entities. These measures are designed to ensure that critical entities can effectively manage and mitigate risks, thereby maintaining the continuity of essential services.
- Risk assessments: both Member States and critical entities are required to conduct regular risk assessments. These assessments must consider all relevant risks, whether natural or man-made, that could disrupt the provision of essential services. Member States must report their findings to the European Commission
- Incident notification: critical entities must notify competent authorities within 24 hours of becoming aware of significant incidents that disrupt or could disrupt the provision of essential services. The notification should include details such as the number of affected users, the duration of the disruption, and the geographical area impacted.

Difference between the CER Directive and NIS2 Directive

The CER and NIS2 Directives both aim to enhance the resilience of critical entities in the EU but focus on different aspects.

The NIS2 Directive is specifically oriented towards cybersecurity, targeting essential and important entities to ensure robust cyber defenses and reporting. In contrast, the CER Directive takes a broader approach, addressing both physical and cyber threats. It does not distinguish between “essential” and “important” entities, instead referring to “critical entities” and covering a wide range of sectors, including energy, transport, banking, healthcare, and digital infrastructure.

Entities identified as critical under the CER Directive should also be considered essential under the NIS2 Directive. Therefore, both pieces of legislation will be applicable to these entities. Critical entities under the CER Directive must comply with the cybersecurity risk management measures and reporting obligations imposed by the NIS2 Directive. To streamline supervisory activities and minimize the administrative burden, competent authorities should harmonize incident notification templates and supervisory processes.

The CER Directive does not apply to cybersecurity matters covered by the NIS2 Directive. Thus, essential or important entities that are also critical under the CER Directive will only be subject to the CER Directive for issues beyond the scope of the NIS2 Directive. An exception exists for the digital infrastructure sector, due to its importance to other sectors. Member States should identify digital infrastructure entities as critical and apply the relevant CER Directive strategies, risk assessments, and support measures.

Further reading

For further reading on the NIS2 Directive and our EI-wide implementation tracker, please be referred to our NIS2 landing page.