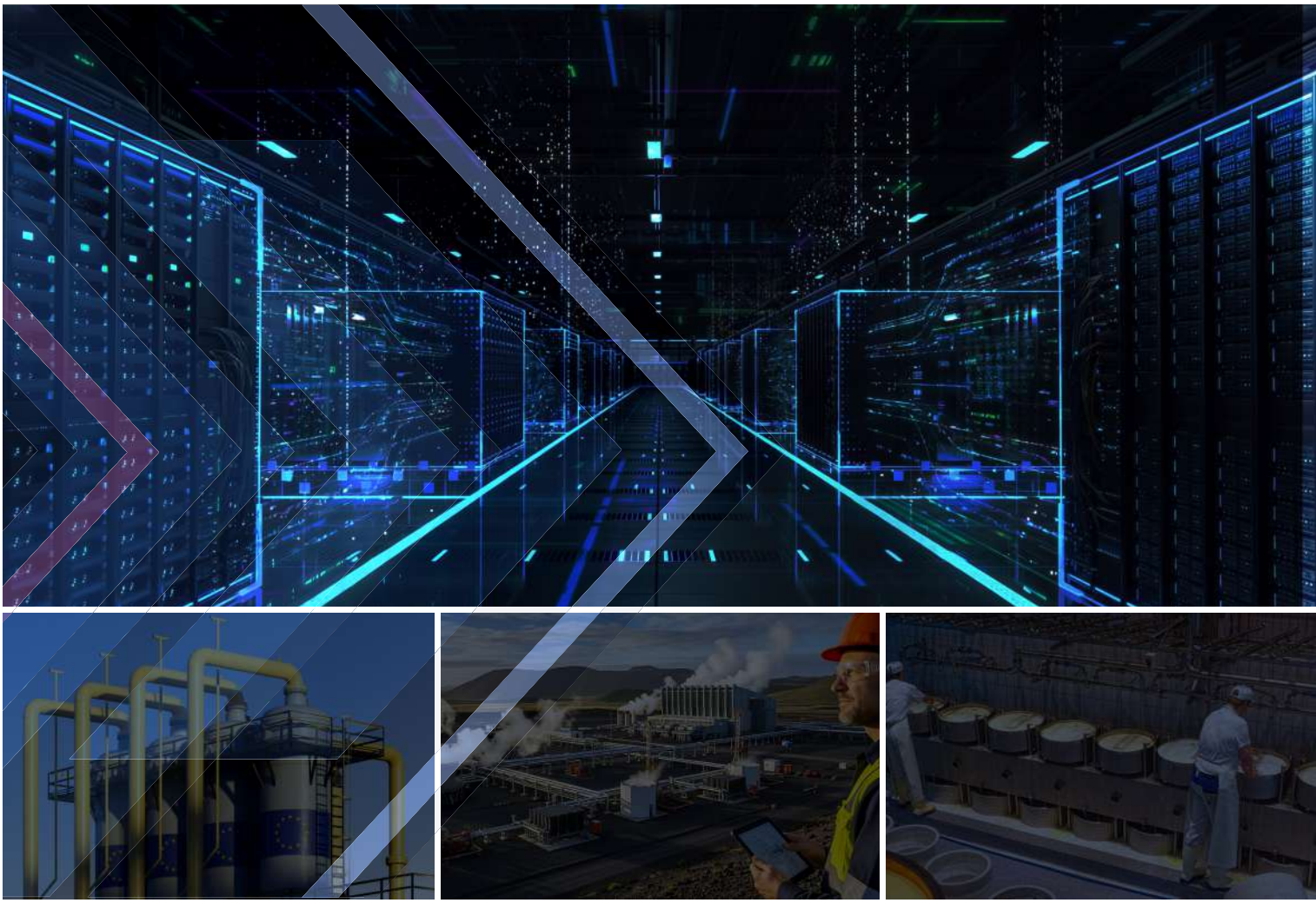
KNYRIM.TRIEB
ATTORNEYS AT LAW

INTERNATIONAL SOS
CONSULTING

THE CER DIRECTIVE:
FROM COMPLIANCE TO CRISIS READINESS

How organisations across 11 critical sectors can turn regulatory obligation into operational resilience before the July 2026 deadline.



EXECUTIVE FOREWORD: THREE PERSPECTIVES

Gautier Porot
Global Crisis Management
Practice Leader,
International SOS

Critical entities now operate in an environment defined by interdependence, volatility, and scrutiny. This paper is most relevant to organizations that provide essential services in one of the 11 sectors covered by the Directive, including energy, transport, banking, health, digital infrastructure, water, public administration, space and food, and that may be designated by a Member State as a "critical entity" because disruption would significantly affect those services. It is therefore not about all companies, but about those whose operations are especially important to the continuity of essential services.

What has changed since the earlier European framework is not simply the number of sectors covered, but the nature of the problem itself: resilience is no longer about protecting individual assets in isolation, but about sustaining essential services through disruption across physical, operational, and increasingly interconnected systems. That shift matters because failures now rarely remain contained; they cascade across supply chains, sectors, and borders. That is why CER should be read as more than a compliance milestone. It reflects a broader expectation that organizations will be able to show that governance holds under pressure, that dependencies are understood, and that essential services can continue when disruption is no longer theoretical.

Mag. Gregor Brandstetter
BA, Associate,
Knyrim Trieb Attorneys at Law,
Austria

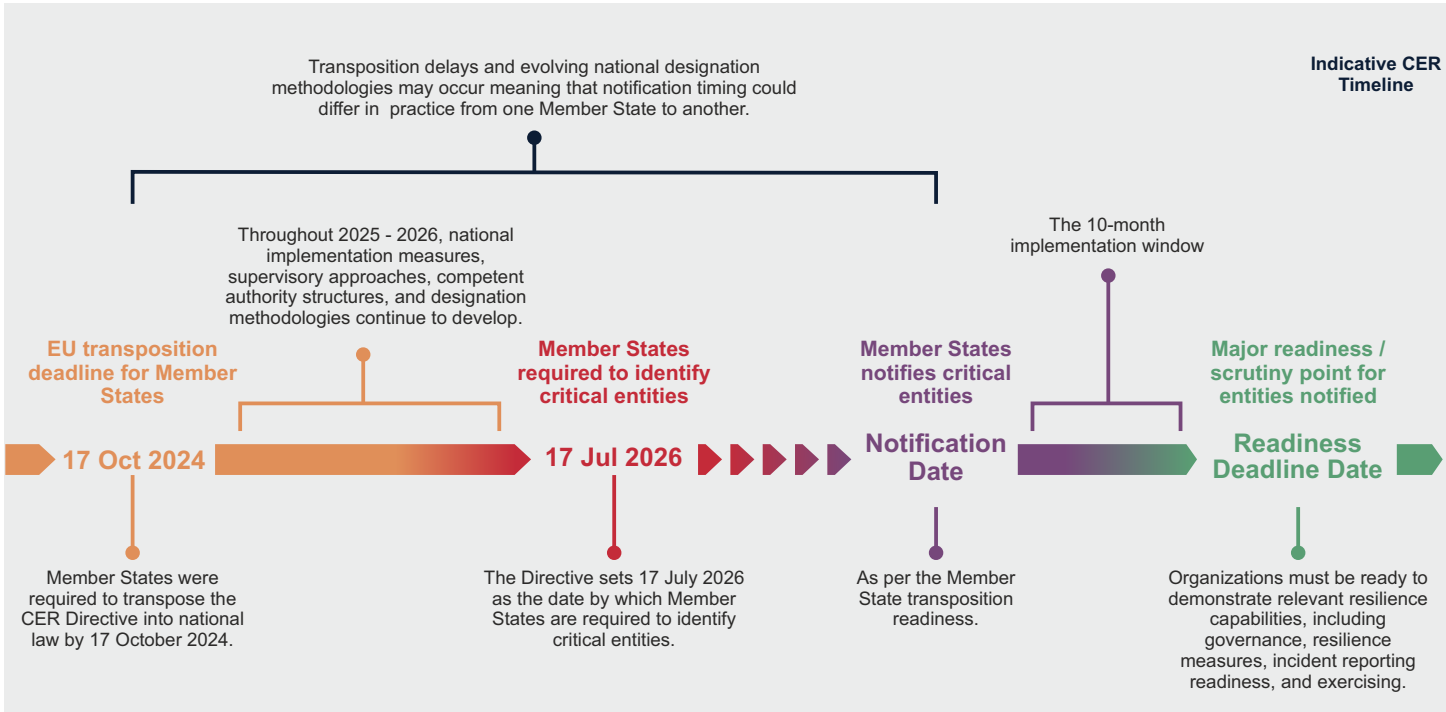
From a legal perspective, CER creates a common European framework but does not create a single, uniform compliance experience for organisations. The Directive becomes enforceable for designated entities through **national implementing legislation**, and that means organisations must pay close attention to transposition status, local designation methodologies, supervisory structures, and reporting expectations in every jurisdiction where they operate. The July 2026 milestone is therefore important, but in practice notification and enforcement timelines may vary from one Member State to another.

Close attention must also be given to the interactions between CER and other frameworks such as NIS2 and, where relevant, DORA. These frameworks are complementary, and in some areas equivalent, but that should not be assumed without careful mapping and evidence. One of the strengths of this paper is that it recognises this legal complexity while keeping the focus on what organisations need to do in practice to prepare.

Audrey Schoehn
Crisis Management
Consultant,
International SOS

The most important resilience gaps rarely appear where organisations expect them to. Plans may exist, ownership may appear clear, and programmes may be underway, yet when disruption begins, the real test is whether decisions are made quickly enough, whether escalation works, whether crisis management and business continuity function together, and whether the organisation knows what it must protect first. That is the difference between documented compliance and operational readiness, and it sits at the heart of this paper.

Organisations that emerge stronger from CER are usually those that treat it not as a separate compliance workstream, but as an opportunity to bring fragmented resilience efforts together under one governance model. They **identify their Minimum Viable Firm, clarify decision rights, map dependencies, test their response, and build the evidence needed to show that capability exists**. This paper is designed to help leaders do exactly that: understand what matters most, where organisations typically struggle, and how to turn resilience expectations into something that works under pressure.



1 CER IN CONTEXT: A COMPLEX REGULATORY LANDSCAPE

Below, when we refer to "recitals", we mean the opening explanatory text of the Directive. Although this text is not legally binding, it helps explain how the main legal requirements should be understood.

1.1 What the Cer Changes

The 2008 European Critical Infrastructure Directive was designed for a threat environment that no longer exists. As a result, the scope of this directive was narrower, covering only energy and transport. Furthermore, the approach focused on assets, specifically on identifying and physically protecting them.

Since 2008, the world has undergone structural changes and developments: pandemics, hybrid threats, 'state-sponsored' sabotage, climate-related disruptions, and the domino effect within supply chains have all altered and shaped the landscape in such a way that it is now fundamentally different from that of 2008. The 2008 Directive ultimately proved insufficient.

The fundamental change brought about by the CER is explicitly stated in Recital 2: the emphasis moves from protecting individual assets to sustaining the provision of essential services through disruption. This is not merely a semantic distinction; it reflects a drastic shift in the elements to be assessed and protected, and above all, in what the organisation is responsible for.

This directive (CER) broadens its scope to such an extent that it now covers not two sectors but 11: energy/ transport/ banking/ financial market infrastructure/ health/ drinking water/ wastewater/ digital infrastructure/public administration/ space/ production, processing & distribution of food. It adopts an 'all-risk' approach, effectively incorporating natural disasters, pandemics and accidents, so as not to be limited to a single category of risk.

A less prominent but operationally significant requirement within art.13 concerns external service providers: entities must account for their staff when mapping critical functions. This is a legal obligation, though one that is frequently underestimated. An organisation's resilience depends on that of the entities with which it is in contact; conversely, a service provider's resilience depends in part on the organisation it supplies. Identifying and mapping dependencies is not only a legal requirement but also, as we have observed over the past 40 years, one of the most revealing operational exercises a critical entity can undertake.

1.2 Who is a Critical Entity?

Designation as a critical entity requires the fulfilment of three cumulative criteria under Art.6(2): the organisation provides an essential service, it operates within the territory of a European Member State, and an incident affecting it would result in a significant disruption to the service provided (assessed using the criteria set out in Art.6).
The criteria set out in Art.7 enable self-assessment: these include the number of users dependent on the service, cross-sector dependencies, the geographical scope of the potential disruption, market share, and the availability of substitutes for the organisation. Organisations whose specific characteristics meet multiple criteria should regard designation as a serious possibility rather than a contingency requirement.

Once designated, four key requirements apply: the implementation of risk assessment, resilience measures, incident reporting and exercises. Each requirement has its own timeline and deadline for implementation, as set out in section 3.

Concept	CER Definition (Art.2)
Critical entity	Public or private entity designated by a Member State under Art.6 as belonging to one of the Annex categories
Resilience	Ability to prevent, protect against, respond to, resist, mitigate, absorb, accommodate and recover from incidents
Incident	Event that disrupts or is capable of significantly disrupting the provision of an essential service
Essential service	Service crucial for the maintenance of vital societal functions, economic activities, public health, public safety or the environment
Risk	Potential for loss or disruption caused by an incident, expressed as a combination of magnitude and likelihood of occurrence of the incident

1.3 The Regulatory Landscape: CER, NIS2, DORA

Many organisations may fall under more than one framework. The interaction between CER, NIS2 and DORA is one of the most common sources of confusion we encounter in client discussions.

Framework	Focus	Equivalence
CER	Physical and operational resilience	Reference framework
NIS2	Cybersecurity and network resilience	Recognised (Art.1(2) + Art.8)
DORA	Digital operational resilience (financial sector)	Recognised (Recital 21)

Where sector-specific EU law imposes equivalent requirements, certain CER obligations may not apply (Art.1(3) & Recital 10), provided equivalence is formally recognised and documented. For organisations already subject to DORA or NIS2, this creates a genuine opportunity to build on existing investments rather than duplicate them. However, equivalence must be mapped and evidenced; it cannot simply be assumed.

> " It is important to understand, however, that recognition does not imply approval: a detailed mapping of requirements is often necessary. Equivalence must be assessed for each measure."
>
> KNYRIM.TRIEB ATTORNEYS AT LAW

The reason for regulatory multiplicity and complexity within an organisation lies not only in duplication but also in fragmentation; the CER Directive might be assigned to the legal department, NIS2 to IT security and DORA to the CFO's office: with no single owner and, above all, without a full understanding of what each programme requires of the others. Gaps may, for example, arise at the intersection of physical and cyber resilience: this is also the point that is being scrutinised closely by the competent authorities.

1.4 National Transposition Uncertainty

Although the CER Directive establishes a common European framework, organisations should avoid assuming that implementation will be fully harmonised across Member States. At the time of writing, national transposition remains incomplete in many jurisdictions and several key elements are still evolving.

Designation methodologies, supervisory approaches, reporting expectations, competent authority structures and sanctioning regimes are likely to differ significantly between Member States. As a result, the practical compliance target remains partially unsettled.

> "A common EU framework does not mean identical national application. For multi-jurisdiction organisations, timelines and supervisory expectations may diverge."
>
> KNYRIM.TRIEB ATTORNEYS AT LAW

For organisations operating across multiple jurisdictions, CER compliance should therefore be approached as a moving target rather than a fixed checklist. Early engagement with national implementation measures and competent authorities will be as important as understanding the Directive itself.

2 THE READINESS GAP: WHY COMPLIANCE ON PAPER IS NOT ENOUGH

In the organisations we work with, readiness gaps rarely emerge where management expects them to. Whilst risk registers are often robust and resilience plans well-structured, what often breaks down first is decision-making itself: who needs to be brought together, with what authority, based on what information, and within what timeframe. The CER's definition of resilience in eight verbs implicitly tests this.

The directive itself implicitly acknowledges this. Art.13(2) requires critical entities to apply their resilience plan; simply writing it down is not enough.

> "Application" is the key word and carries considerable weight. Indeed, this implies that even if a document is beautifully drafted but is not linked to the way in which the executive committee actually makes decisions under pressure, it will not satisfy a competent authority for long; moreover, it will be of no use whatsoever when a crisis arises."
>
> INTERNATIONAL SOS CONSULTING

Four structural factors are constantly widening the gap between documented compliance and operational preparedness:

Increasing Complexity of Threats

Recitals 2 to 5, contained in the preamble to the Directive, explicitly list natural hazards, climate risk, hybrid threats, terrorism and supply chain disruptions. The all-hazards approach adopted by the Directive is not merely rhetorical; it establishes the basis on which risk assessments will be conducted and against which incidents will ultimately be measured.

Organisational Silos

The CER's multi-risk and deliberately cross-functional approach aims to re-establish the link and overcome the fragmentation between physical, IT, legal, HR and operational security. This is one of the major risks of the drive for compliance: some organisations will produce only compliant documents but no real capacity for resilience.

Unmanaged Dependencies

Section 2 of Art.12 establishes cross-border and cross-sector dependency mapping as a legal obligation. In practice, however, most organisations have only a partial view of their critical dependencies, suppliers, third-party technology providers, regulatory relationships and key individuals, and a very incomplete view of second-order dependencies. This lack of awareness prevents a comprehensive mapping of risks, let alone the implementation of sufficient measures to mitigate these risks.

Limited Crisis Culture

Art.13(1)(f) requires that staff be informed of resilience plans and trained through exercises. Thus, employees' understanding of a company's resilience capabilities is not based solely on a recommendation of best practice. Furthermore, the shortcoming we most frequently observe is not the absence of exercises, but rather the absence of challenging exercises. Indeed, whilst a simulation designed to confirm that the plan works is a positive step, it is not sufficient. A best practice observed is to create challenging scenarios and seek to identify points of failure (decision-making, reporting the incident or crisis to the authorities, etc.); this type of simulation builds resilience because it challenges a plan that might have been thought to be perfect.

The Multi-Jurisdictional Reality

For organisations operating in several EU Member States, the CER introduces a level of complexity that planning for a single jurisdiction cannot resolve. Designation letters will not arrive simultaneously. National transpositions differ in terms of threshold criteria, compliance deadlines and the intensity of supervision.

For a group operating in five or eight Member States, the practical questions are: which designation do you prioritise, who coordinates across jurisdictions, how do you manage conflicting national requirements, and how do you present a coherent resilience architecture to multiple competent authorities?

These are questions that often require deliberate design beyond a centrally managed compliance programme.

3 WHAT CER ACTUALLY REQUIRES: FIVE KEY DIMENSIONS

The directive uses phrases such as ‘appropriate and proportionate’ and ‘without undue delay’, which are deliberately flexible yet still binding. This scope for interpretation is both an opportunity and a risk. It allows organisations to build on existing programmes rather than starting from scratch. However, relying too heavily on pre-existing arrangements that no longer meet the Directive's requirements can create compliance gaps. Limited investment may appear sufficient until an incident or inspection exposes the shortfall.

Risk Assessment (Art.12) - Nine-Month Deadline Post-Designation

The risk assessment requirement, as set out in Art.12 of the Directive, has four distinctive features:
According to the recital 28 and Art.12(2), all risks, whatever their nature, must be considered : natural, accidental, man-made or hybrid hazards. A risk assessment that addresses only historically prioritised hazards, threats and risks will not be sufficient for the purposes of the Directive unless it is revised and supported by documented evidence demonstrating the absence of additional risks.

This risk assessment must map dependencies, whether they are cross-sectoral, cross-border interdependencies, including those involving other Member States and third countries (Art.12(2)). This is where the obligation becomes most demanding for organisations with complex supply chains or multi-jurisdictional operations.

The risk assessment may draw on existing work: the competent authorities may recognise equivalence with risk assessments carried out in connection with other EU obligations (Art.12(2)). It is advisable to proactively document this equivalence in order to demonstrate that compliance efforts are aligned with the Directive.

> “Risk assessment is not a one-off exercise."
>
> INTERNATIONAL SOS CONSULTING

Risk Assessments must be maintained and periodically reviewed: at least every four years or whenever the organisation has undergone a significant change or a major incident (Art.12(1)).

A meaningful risk assessment under Art.12 requires a prior answer to a question that the Directive does not explicitly ask but implicitly presupposes: what, precisely, must not fail? Without this decision-making anchor, risk assessments tend towards comprehensiveness at the expense of prioritisation; the aim is not to produce documents that identify everything but protect nothing decisively.

Resilience Measures (Art.13) - Ten-Month Deadline Post-Designation

Art.13 sets out six resilience measures: prevention, physical protection, crisis response and mitigation, business continuity and recovery planning, staff safety, and staff training and drills.
To ensure the safety of staff and assets, Art.14 allows organisations to request background checks on staff in sensitive roles, including criminal record checks via the EU’s ECRIS system. To date, this capability is little known and consequently underused by many organisations that have not integrated it into their HR and security frameworks.

Existing resilience plans linked to other legal obligations, which may meet the requirements of Art.13 (see the six resilience measures) and which have been declared by a competent authority to comply with those requirements (with documented and defensible equivalence), may be retained.
Each entity must appoint a liaison officer to act as the point of contact with the competent authorities (Art.13(3)). Beyond a formal governance requirement, the role carries real operational weight: responsibility for ensuring 24/7 notification capability and supporting inspections.

Incident Reporting (Art. 15) - Real-Time Obligation

Incident reporting is one of the Directive's most operationally demanding requirements. Significant incidents must be notified within 24 hours of becoming known, to the competent authority, followed by a detailed report within one month. The significance of an incident is assessed on the basis of the number of users affected, the duration and the geographical scope (Art.15(1)).

In practice, it is at the time of the initial notification (within 24 hours) that most organisations discover that their escalation chain has been designed and organised for normal operations and not for out-of-hours situations. Those that consistently comply are rarely the organisations with the most detailed procedures; they are the ones that have exercised under pressure, assigned responsibility to roles rather than individuals (allowing for deputies), and tested communication channels with competent authorities in advance.

> “Detection capabilities, escalation procedures, decision-making authority at every stage, and pre-approved communication templates are not mere luxuries of preparedness; they form the infrastructure that enables round-the-clock notification.”

Governance & Accountability (Art. 13)

CER's governance requirements are explicit and senior. The resilience programme must be formally governed, regularly reviewed and owned at executive level. Art.13 requires critical entities to establish crisis management, business continuity and recovery capabilities, while ensuring that relevant personnel are trained and exercised. Where strategic decisions would ultimately rest with board members or senior executives, excluding them from resilience exercises creates a significant gap between documented governance and operational capability. The implementation and maintenance of resilience measures under Art.13 require active executive oversight and clear accountability arrangements.
The question competent authorities will ask is not whether a plan exists, but whether the people named in it can actually execute it under pressure.

Sanctions (Art. 22) and Supervision (Art. 21)

Art.22 requires Member States to establish sanctions that are ‘effective, proportionate and dissuasive’. Unlike GDPR, no EU-wide cap exists, creating significant variation between Member States. Early national transpositions suggest that financial penalties may become material for some organisations. Member States will also be required to notify the Commission of any changes made to this system of sanctions.
The supervisory powers set out in Art.21 are extensive and include on-site inspections, remote monitoring, audits and binding remedial orders. For entities operating in six or more Member States that provide the same or similar essential services, Art.17-18 create an additional layer of supervision at EU level. Formal designation as a critical entity of particular European significance triggers advisory missions and coordination mechanisms extending beyond any single national authority. In practice, fines rarely become the main concern. Operational disruption and reputational damage usually dominate executive discussions after a serious incident.

What CER Readiness Looks Like in Practice

Before examining how crisis management translates CER obligations into operational capability, it is worth pausing to describe what a genuinely CER-ready organisation looks like in practice, not on paper, but in the room when it matters.

A CER-ready organisation is not defined only by the existence of plans or policies, but by whether resilience can be demonstrated in practice. In operational terms, “good” typically looks like this:

- **Governance is clear:** executive ownership visible, decision rights defined, accountability documented.
- **The incident reporting chain works:** tested escalation path, role-assigned responsibilities, 24-hour capability confirmed.
- **Critical functions are identified:** the MVF is mapped at the level of processes, people and relationships.
- **Exercising is active and meaningful:** simulations designed to reveal friction, not confirm existing plans.
- **Dependencies are mapped:** cross-sector, cross-border and third-party dependencies inform risk assessment and response.
- **Evidence is organised:** supporting materials documented and explainable under scrutiny.

4 CRISIS MANAGEMENT AS THE ENGINE OF CER COMPLIANCE

The CER Directive requires operational capability, not merely documentation. The use of the word "apply" in Art.13(2) is deliberate; it indicates that the competent authorities are likely to focus on whether resilience measures can be demonstrated in practice."

The definition of resilience using eight verbs in Art.2(2) corresponds directly to the crisis management cycle:

CER Obligation	Art. Reference	Practical Translation
Systemic risk assessment	Art.12	All-hazard, dependency mapping, MVF identification
Clear governance	Art.13	Board ownership, liaison officer, decision authorities
Actionable procedures	Art.13	Applied resilience plan, not filed
Communications (internal and external)	Art.15	24h reporting, stakeholder communications
Regular exercises	Art.13(1)(f)	Legal obligation, not best practice
Post-incident review	Art.12	Feeds the four-year review cycle

Organisations frequently confuse resilience planning with resilience capability. A plan describes what should happen. Capacity is what actually happens when the plan meets reality. Art.13 of the CER deliberately uses the word ‘implement’; it requires the latter.

4.1 The Minimum Viable Firm: Operationalising Cer's Core Obligations

The directive uses the terms 'essential services' and 'critical functions' without telling organisations how to identify them internally. That identification is the work the directive does not do for you, and it is where most compliance programmes stall, not identifying the Minimum Viable Firm (MVF).

The MVF is neither a category nor a department; it is the vital core of the business, its viability, the specific intersection of flows, assets and relationships without which the organisation cannot rebuild itself within an operationally or commercially viable timeframe. Identifying it requires a level of granularity that risk assessments conducted at sector or function level generally do not achieve.

> “It is worth noting that the MVF is a distinct concept from the CER's definition of 'essential services'. The latter is a regulatory designation determined externally by competent authorities; the MVF is an internal analytical tool, more granular focused, that helps organisations decide where to concentrate their resilience investment.”

Identifying the MVF is the basis for meaningful compliance with the CER for two specific reasons:

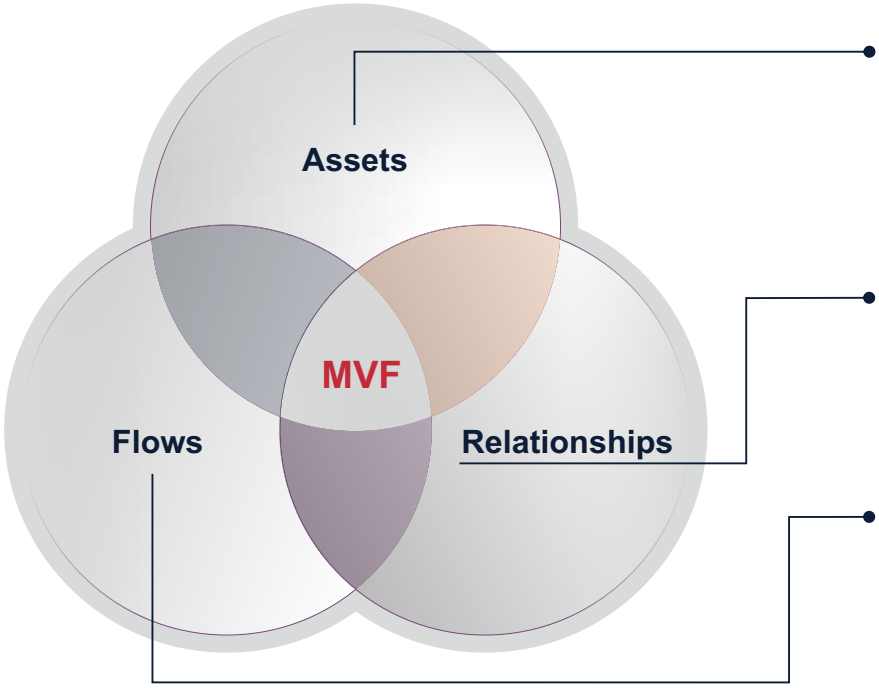
Regarding Art.12 (Risk Assessment):

A risk assessment that attempts to be exhaustive without a framework for prioritisation tends to result in exhaustive documentation and diffuse protection. The MVF provides this framework. It defines which elements must be preserved and which can be set aside for a time. This distinction is what makes the ‘significant disruptive effect’ within the meaning of Art.7 analytically defensible rather than subjective.

For Art.13 (Resilience Measures):

The Directive requires ‘appropriate and proportionate’ measures. Proportionality, in practice, requires knowing what the measure is proportionate to. Without MVF identification, proportionality becomes a judgement made under resource pressure rather than a principled and auditable position. With the help of the MVF, the logic is clear: measures protecting the vital core are non-negotiable; measures protecting the degradable layers are calibrated according to recovery objectives and resource constraints. This is an approach that stands up to both inspection and an incident.

The MVF is structured around three dimensions, each of which corresponds directly to the CER’s obligations regarding risk assessment and resilience planning:



The people and resources whose loss would make reconstruction impossible or too slow. These are not necessarily the most experienced individuals. They possess tacit knowledge, act as guarantors of decision-making legitimacy in chaotic conditions, and are the assets for which no market substitute exists within an operationally relevant timeframe.

External stakeholders whose support remains intact. A client accounting for a large proportion of turnover, a regulator whose authorisation is required to operate, a technology partner whose failure would paralyse core systems. The crisis constantly reveals that certain relationships are existential, and that no one had formally identified them as such.

The two or three processes whose complete disruption would be irreversible. These are not the most important processes, but those that are essential to the organisation’s survival: decision-making frameworks, critical data flows and strategic connectors, without which the organisation would cease to function.

5 FROM COMPLIANCE TO READINESS: THE PRACTICAL PROGRAMME

The steps below follow the sequence in which decisions actually need to be made, starting before designation, not after.

1 Diagnosis - Art.6, Art.1(3)

Assess designation likelihood. Map existing investments (DORA, NIS2, ISO 22301) against CER requirements. Identify gaps, equivalences and applicable national transpositions.

2 Identify the MVF – CER: Art.12, Art 13

(should be done even if not designated)

Define essential services with CER-level precision. Map critical functions, vital dependencies, and the specific processes, people and relationships forming the vital core.

3 Governance and Structure – CER Art.13(1,3)

Appoint liaison officer. Establish crisis governance structure: decision authorities, escalation procedures. Organisations should assess whether board members and senior executives need to participate given their crisis decision-making responsibilities (board engagement).

4 Procedures and Manuals – CER Art.13(2), Art.15

Develop or update resilience plan. Build 24h notification chain (role-assigned). Draft communication templates for authorities and key stakeholders.

5 Training and Exercises: Art.13(1)(f)

Run stress-test simulations designed to reveal failure points, not only confirm existing plans. Include decision-makers. Legal obligation, not best practice.

6 Documentation and Evidence – Art.12, Art.13, Art.21

Compile resilience evidence file: risk assessment, resilience plan, exercise records, post-action reviews, incident reporting procedures, liaison officer designation, equivalence mapping.

Indicative Evidence Organisations Should Be Ready to Demonstrate

None of these elements need to be created from scratch, but they do need to exist, to be coherent, and to be explainable under scrutiny. Precise requirements will depend on national implementation and competent authority expectations.

Risk Assessment:
current, all-hazard, with dependency mapping and documented review triggers.

Resilience Plan:
showing how the six Art.13 measures are being implemented.

Governance Records:
executive ownership, decision authority, escalation paths.

Liaison officer:
designated, operationally embedded, not nominal.

Incident Reporting Procedure:
tested process with roles, approvals and communication templates.

Exercise and Training Records:
including lessons identified and actions taken.

After-Action Reviews:
showing how findings feed back into resilience improvements.

Equivalence Mapping (where Relevant):
NIS2/DORA investments mapped against CER obligations and documented.

6 RESILIENCE READINESS SELF-ASSESSMENT

The following assessment is structured to give organisations a rapid but honest view of their current readiness position. Score each question as stipulated in the table below.

Scoring guide:

- 0–5: Compliance exposure: designation is likely to create immediate audit risk; prioritise Steps 1–3 of the programme above
- 6–9: Structured but untested: documentation exists; operational readiness is unverified; prioritise Steps 4–5
- 10–16: Readiness foundation: gaps are known and manageable with targeted investment; focus on evidence and exercise quality

Question	Yes= 2	Partially= 1	No= 0	Priority	Signal if “No” or “Partially”
Have you assessed whether your organisation meets the Art.6(2) criteria for designation?				High	You are making resilience investment decisions without knowing whether they will be subject to regulatory scrutiny.
Have you formally identified your Minimum Viable Firm (the specific processes, people and relationships)whose disruption would make recovery impossible?				High	Your risk assessment has no prioritisation anchor. "Appropriate and proportionate" measures under Art.13 cannot be defined without it.
Could your organisation issue an incident notification to the competent authority within 24 hours today?				High	Your escalation chain was likely designed for normal operations. The 24-hour clock does not adjust for organisational complexity.
Is crisis management formally owned at board or C-suite level, with active participation, not delegation?				High	Where boards retain crisis decision-making authority, excluding them from exercises may create a significant governance gap. Ownership that exists only on an organisation chart is not ownership.
Have you mapped your critical dependencies: suppliers, third-party technology, key individuals, cross-border links?				High	Art.12(2) makes dependency mapping a legal obligation. Unmapped dependencies are the failure paths that crises exploit.
When was your last crisis simulation or resilience exercise?				Medium	If the answer is more than 12 months ago, or if the exercise was designed to confirm the plan rather than stress-test it, the capability is unverified.
Are your CER, NIS2 and DORA workstreams coordinated under a single resilience owner?				Medium	Parallel, uncoordinated programmes burn budget, fragment accountability and leave gaps at the seams between physical and cyber resilience.
Have you designated a liaison officer under Art.13(3), or established a plan to do so?				Medium	The liaison officer is the individual legally responsible for 24-hour notification and the primary interface during inspections. This role cannot be improvised.
Are your existing DORA or NIS2 investments formally mapped against CER obligations to document equivalence and avoid duplication?				Medium	Equivalence under Art.1(3) is available but must be demonstrated, not assumed. Undocumented equivalence is no equivalence at all.
Does your resilience plan reflect your multi-jurisdictional footprint, including divergent national timelines, thresholds and supervision intensity?				Medium	For multinationals, designation letters will not arrive simultaneously and will not say the same thing. A single-jurisdiction plan is a partial plan.

7 CONCLUSION

CER reflects regulatory recognition of a fundamental shift in the risk landscape. The organisations that navigate this most successfully will not be those that produce the most comprehensive compliance documentation, but those that use the directive's requirements as a framework, a model for building and maintaining a capacity for resilience capable of withstanding both an inspection and an incident.

The timetable is set. By 17 July 2026, Member States are required to have identified their critical entities, though, as noted, notification timelines will vary in practice. From the date of notification, the ten-month compliance window moves quickly. Organisations that begin preparations before designation, mapping their MVF, aligning their governance, testing their incident reporting chain, will find the window manageable. Those who wait for a designation letter may find the compliance window far less forgiving.

Three points are worth noting from reading this document. Resilience is an executive discipline: as soon as it is delegated, it diminishes, and narrow resilience breaks down first. The quality of decisions in a crisis is determined several months before the crisis, not by plans, but by trust, repeated habits and clear lines of authority established within the leadership team. And the gap between documented compliance and operational readiness is real, yet measurable and, with deliberate effort, bridgeable.

This document provides a general overview of the EU Critical Entities Resilience Directive (EU) 2022/2557 and is intended for informational purposes. It does not constitute legal or regulatory advice. Organisations should seek appropriate guidance based on their specific circumstances and the applicable national implementing legislation.

AUTHORS

Mag. Gregor Brandstetter, BA,
Associate at Knyrim Trieb Rechtsanwälte OG

Gautier Porot
Global Crisis Management Practice Leader at International SOS

Audrey Schoehn
Crisis Management Consultant at International SOS