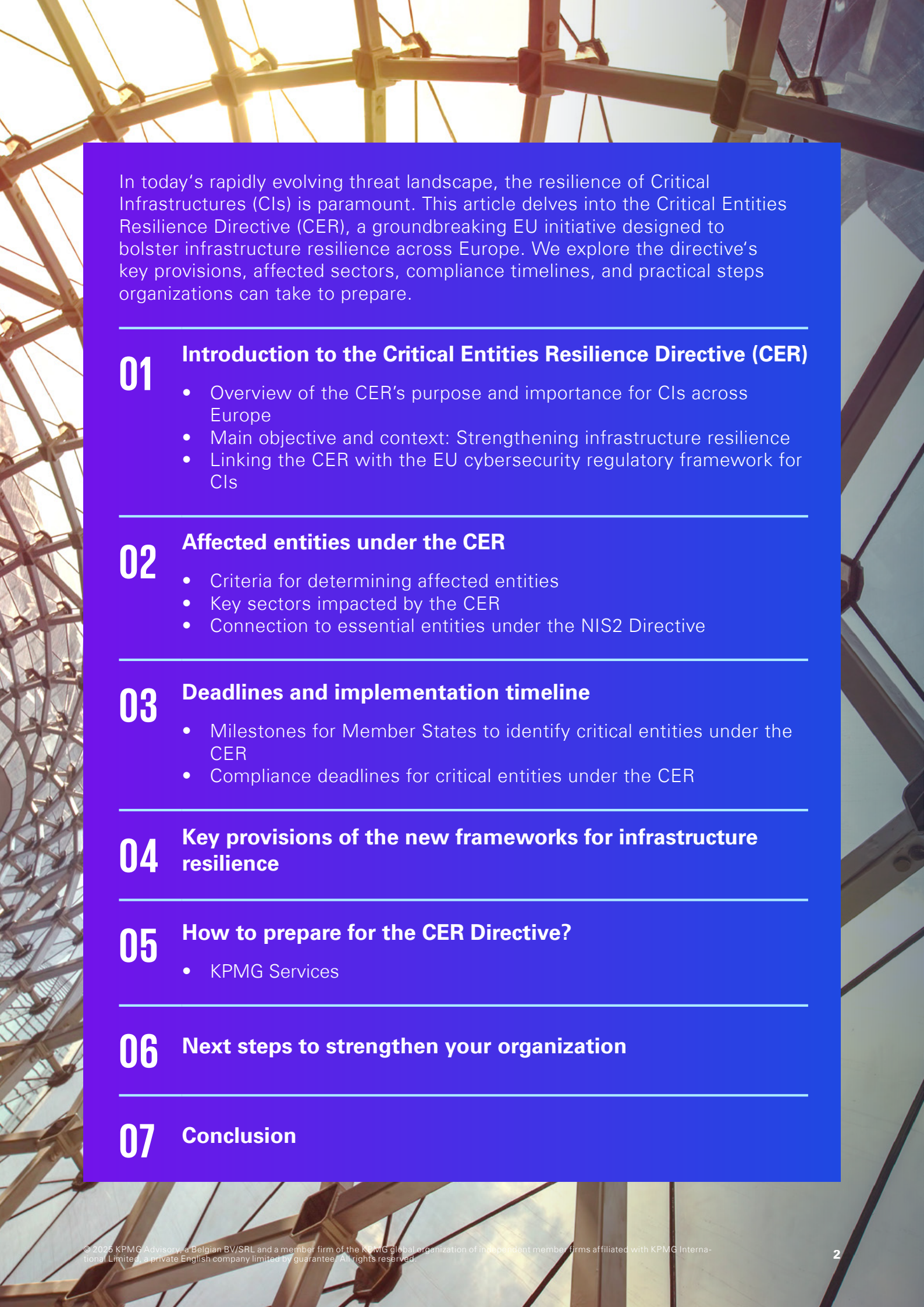




Enhancing infrastructure resilience across Europe

An in-depth analysis of the new
Critical Entities Resilience
Directive (CER) and its impact
on your organization



In today's rapidly evolving threat landscape, the resilience of Critical Infrastructures (CIs) is paramount. This article delves into the Critical Entities Resilience Directive (CER), a groundbreaking EU initiative designed to bolster infrastructure resilience across Europe. We explore the directive's key provisions, affected sectors, compliance timelines, and practical steps organizations can take to prepare.

01 Introduction to the Critical Entities Resilience Directive (CER)

- Overview of the CER's purpose and importance for CIs across Europe
- Main objective and context: Strengthening infrastructure resilience
- Linking the CER with the EU cybersecurity regulatory framework for CIs

02 Affected entities under the CER

- Criteria for determining affected entities
- Key sectors impacted by the CER
- Connection to essential entities under the NIS2 Directive

03 Deadlines and implementation timeline

- Milestones for Member States to identify critical entities under the CER
- Compliance deadlines for critical entities under the CER

04 Key provisions of the new frameworks for infrastructure resilience

05 How to prepare for the CER Directive?

- KPMG Services

06 Next steps to strengthen your organization

07 Conclusion



1. Introduction to the Critical Entities Resilience Directive (CER)

1.1 Overview of CER's purpose and importance for CIs across Europe

The CER stands as a landmark legislative initiative aimed at fortifying the resilience of CIs and essential services throughout Europe. As vulnerabilities in critical systems continue to pose significant risks to national security, public safety, and economic stability, the CER emerges as a proactive response to mitigate these risks and ensure the uninterrupted operation of vital services.

The importance of the CER transcends regulatory compliance; it underscores the critical need to enhance the preparedness and response capabilities of CIs operators in the face of a dynamic and evolving threat landscape. By fostering a culture of resilience and accountability, the directive catalyzes a paradigm shift towards proactive risk mitigation, adaptive planning, and collaborative engagement among stakeholders across various sectors.

The CER fosters cross-border coordination and information sharing among European countries, thereby promoting a collective approach to managing risks and ensuring the interoperability of CIs systems. Through alignment with best practices, industry standards, and emerging technologies, the directive propels organizations towards a state of operational excellence, where resilience becomes ingrained in their organizational DNA.

In essence, the CER embodies a forward-looking vision to elevate the resilience posture of CIs across Europe, laying the foundation for a secure, reliable, and interconnected infrastructure network that can weather disruptions with resilience and agility.

1.2 Main objective and context: Strengthening infrastructure resilience

In a rapidly changing and interconnected world, where threats to infrastructure resilience are becoming more complex and pervasive, the CER provides a structured approach to fortifying the reliability and continuity of essential services. Through proactive measures, such as conducting risk assessments, implementing robust contingency plans, and fostering cross-sector

collaboration, the directive aims to build a more resilient and sustainable infrastructure landscape that can withstand unforeseen shocks and maintain operational stability.

1.3 Linking the CER with the EU cybersecurity regulatory framework for CIs

The CER is partially encompassed within the broader EU cybersecurity regulatory framework for CIs, serving as a cornerstone that contributes to strengthening the resilience and security of essential systems across Europe.

While the CER focuses on strengthening the overall resilience of CIs, the EU cybersecurity regulatory framework specifically addresses cybersecurity measures aimed at safeguarding critical systems from cyber threats and attacks.

When we refer to the **EU cybersecurity regulatory framework** potentially interconnected with the **CER**, we list in a non-sequential order:

1. Network and Information Security (NIS2)

Directive: The NIS2 Directive is an update to the original NIS Directive, aiming to enhance the cybersecurity resilience of essential and important entities across the EU. It expands the scope of sectors covered, introduces stricter security and incident reporting requirements, and enforces stronger supervisory measures and penalties for non-compliance.

2. Digital Operational Resilience Act (DORA):

DORA focuses on ensuring the operational resilience of financial entities against ICT-related risks. It establishes uniform requirements for managing ICT risks, including governance, risk management, incident reporting, and oversight of critical third-party service providers to strengthen the stability of the financial system.

3. Cyber Resilience Act (CRA):

The Cyber Resilience Act introduces mandatory cybersecurity requirements for products with digital elements throughout their lifecycle. It aims to reduce vulnerabilities, prevent cyber incidents, and protect users by establishing standards for secure software and hardware development, vulnerability management, and compliance obligations for manufacturers and suppliers.

4. AI Act:

The AI Act is a regulatory framework that classifies artificial intelligence systems based on their risk levels, ranging from minimal to unacceptable risk. It imposes specific requirements on high-risk AI systems, including transparency, risk management, and accountability measures, to ensure that AI technologies deployed in the EU are safe, ethical, and respect fundamental rights.



CER

The CER Directive aims to strengthen the resilience of essential services and sectors, ensuring their continued operation during crises. Its impact on operational resilience includes increased risk management requirements, enhanced continuity planning, stronger governance, and mandatory reporting. The CER Directive raises the bar for operational resilience by ensuring that critical entities are better prepared, more accountable, and more integrated into a broader resilience framework.

NIS2

The Network and Information Systems Directive 2 (NIS2) strengthens EU-wide cybersecurity by expanding its scope to critical sectors like healthcare, energy, and public services. It aims to harmonize standards, enforce risk management practices, and mandate timely incident reporting. Key goals include improving supply chain security, enhancing accountability at the executive level, and fostering cross-border collaboration. The directive ensures a unified and resilient approach to addressing evolving cyber threats.

DORA

The Digital Operational Resilience Act (DORA) is EU legislation that requires financial institutions to strengthen their operational resilience against ICT-related risks through measures for protection, detection, mitigation, and process recovery. The law entered into application on 17 January 2025.

CRA

The Cyber Resilience Act (CRA) is a new EU regulation designed to ensure safer hardware and software through mandatory cybersecurity requirements for manufacturers. The regulation entered into force in December 2024, with the main obligations applying from December 2027.

AI Act

The AI Act is the EU's regulatory framework for Artificial Intelligence, aiming to ensure safety, transparency, and accountability. It classifies AI systems based on risk levels: unacceptable, high, limited, and minimal. The Act bans AI practices that threaten fundamental rights, like social scoring. It promotes trustworthy AI, requiring transparency for generative AI (e.g., ChatGPT). Companies violating the rules face hefty fines. The AI Act is the first comprehensive AI law, setting a global precedent for AI governance.



ISO 22301

This international standard enhances organizational resilience and is applicable to organizations of all types and sizes. It helps them better anticipate and respond to business continuity risks while also identifying opportunities for improvement more effectively.

By aligning these regulatory frameworks, entities operating CIs can unlock synergies that enhance their overall risk management strategies and resilience capabilities. The interconnected nature of these regulations allows organizations to adopt a holistic approach to addressing operational risks, integrating physical, cybersecurity and business aspects into a unified and comprehensive resilience framework.

Entities subject to both the CER and the EU cybersecurity regulatory framework can benefit from synergies in several key areas:

1. **Risk Assessment and Mitigation:** Aligning risk assessment methodologies and integrating cybersecurity risks into resilience planning helps organizations identify and mitigate a wider range of threats to CIs.
2. **Incident Response and Recovery:** Coordinated protocols for both business and cyber incidents enable efficient crisis management, ensuring swift recovery and minimizing disruptions.

3. Information Sharing and Collaboration:

Promoting information sharing and collaboration enhances collective defense, allowing entities to exchange best practices and threat intelligence for improved resilience.

4. Compliance and Reporting Requirements:

Streamlining compliance and reporting across the CER and EU cybersecurity regulatory framework reduces duplication, optimizes resources, and ensures consistent regulatory adherence.

In essence, the convergence of the CER Directive and the EU cybersecurity regulatory framework presents a unique opportunity for entities to create a robust and integrated resilience strategy that effectively addresses the complex landscape of risks facing CIs. By leveraging on the synergies between these regulations, organizations can strengthen their defenses, enhance their response capabilities, and foster a culture of resilience that goes beyond individual regulatory requirements, ultimately ensuring the continuity and reliability of essential services.

2. Affected entities under the CER

As the CER introduce stronger resilience and security requirements, it is crucial to identify which entities fall under its scope. Determining the affected entities involves a set of criteria that encompass various

factors, such as sectoral importance, criticality of services, and potential impact on society and the economy.

2.1 Criteria for determining affected entities

Entities subject to the provisions of the CER Directive are typically those operating CIs and essential services that are vital for the functioning of society and the economy. The criteria for determining these entities often revolve around factors such as:

1. **Criticality of services:** Entities providing services that are essential for the maintenance of societal functions, economic activities, or public safety are deemed critical and fall under the purview of the CER.
2. **Sectoral importance:** Industries and sectors that play a pivotal role in national infrastructure, such as energy, transportation, healthcare, telecommunications, and water supply, are identified as key sectors impacted by the CER.
3. **Interconnectedness and dependency:** Entities that are interconnected with other CIs systems and whose failure could have cascading effects on multiple sectors are considered crucial in the context of resilience planning.



2.2 Key sectors impacted by the CER

Several key sectors across Europe are profoundly impacted by the Critical Resilience Directive, as depicted in the graphic representation below:

Companies and sectors affected

Energy



- **Electricity**
 - Electricity undertakings which carry out the function of “supply”
 - Distribution system operators
 - Transmission system operators
 - Producers
 - Nominated electricity market operators
 - Market participants providing aggregation, demand response, or energy storage services
- **District heating and cooling**
 - Operators of district heating or district cooling
- **Oil**
 - Operators of oil transmission pipelines
 - Operators of oil production refining and treatment facilities, storage, and transmission
 - Central stockholding entities
- **Gas**
 - Supply undertakings
 - Distribution system operators
 - Transmission system operators
 - Storage system operators
 - LNG system operators
 - Natural gas undertakings
 - Operators of natural gas refining and treatment facilities
- **Hydrogen**
 - Operators of hydrogen production, storage, and transmission

Transport



- **Air**
 - Air carriers used for commercial purposes
 - Airport managing bodies, listed airports, and entities operating ancillary installations contained within airports
 - Traffic management control operators providing ATC services
- **Rail**
 - Infrastructure managers
 - Railway undertakings
- **Water**
 - Inland, sea and coastal passenger and freight water transport companies, not including the individual vessels operated by those companies
 - Managing bodies of ports including their port’s facilities and entities operating works and equipment contained within ports
 - Operators of VTS
- **Road**
 - Road authorities responsible for traffic management control, excluding public entities for whom traffic-management or the operation of intelligent transport systems is a non-essential part of their general activity
 - Operators of Intelligent Transport Systems
- **Public transport**
 - Public service operators

Banking



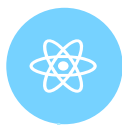
- Credit institutions

Financial market infrastructure



- Operators of trading venues
- CCPs

Health



- Healthcare providers
- EU reference laboratories
- Entities carrying out R&D activities of medicinal products
- Entities manufacturing basic pharmaceutical products and pharmaceutical preparations

Digital infrastructure



- Providers of internet exchange points
- DNS service providers excluding operators of root name servers
- Top-level-domain name registries
- Providers of cloud computing services
- Providers of data center services
- Providers of content delivery networks
- Trust service providers
- Providers of public electronic communication networks
- Providers of electronic communications services

Public administration



- Public administration entities of central governments

Drinking water



- Suppliers and distributors of water intended for human consumption excluding distributors for which distribution of water for human consumption is a non-essential part of their general activity of distributing other commodities and goods

Space



- Operators of ground-based infrastructure, owned, managed and operated by Member States or by private parties, that support the provision of space-based services, excluding providers of public electronic communications networks

Production, processing, and distribution of food



- Businesses which are engaged exclusively in logistics and wholesale distribution and large-scale industrial production and processing

Wastewater



- Undertakings collecting, disposing of or treating urban wastewater, domestic wastewater or industrial wastewater excluding undertakings for which collecting, disposing of or treating urban wastewater, domestic water or industrial wastewater is a non-essential part of their general activity

2.3 Connection to essential entities under the NIS2 Directive

It is essential to note that the entities subject to the CER often align with the concept of 'essential entities' as defined under the NIS2 Directive. **These critical entities, entrusted with providing essential**

services that are paramount for societal well-being, are required to adhere to both the NIS Directive's cybersecurity measures and the resilience provisions outlined in the CER.



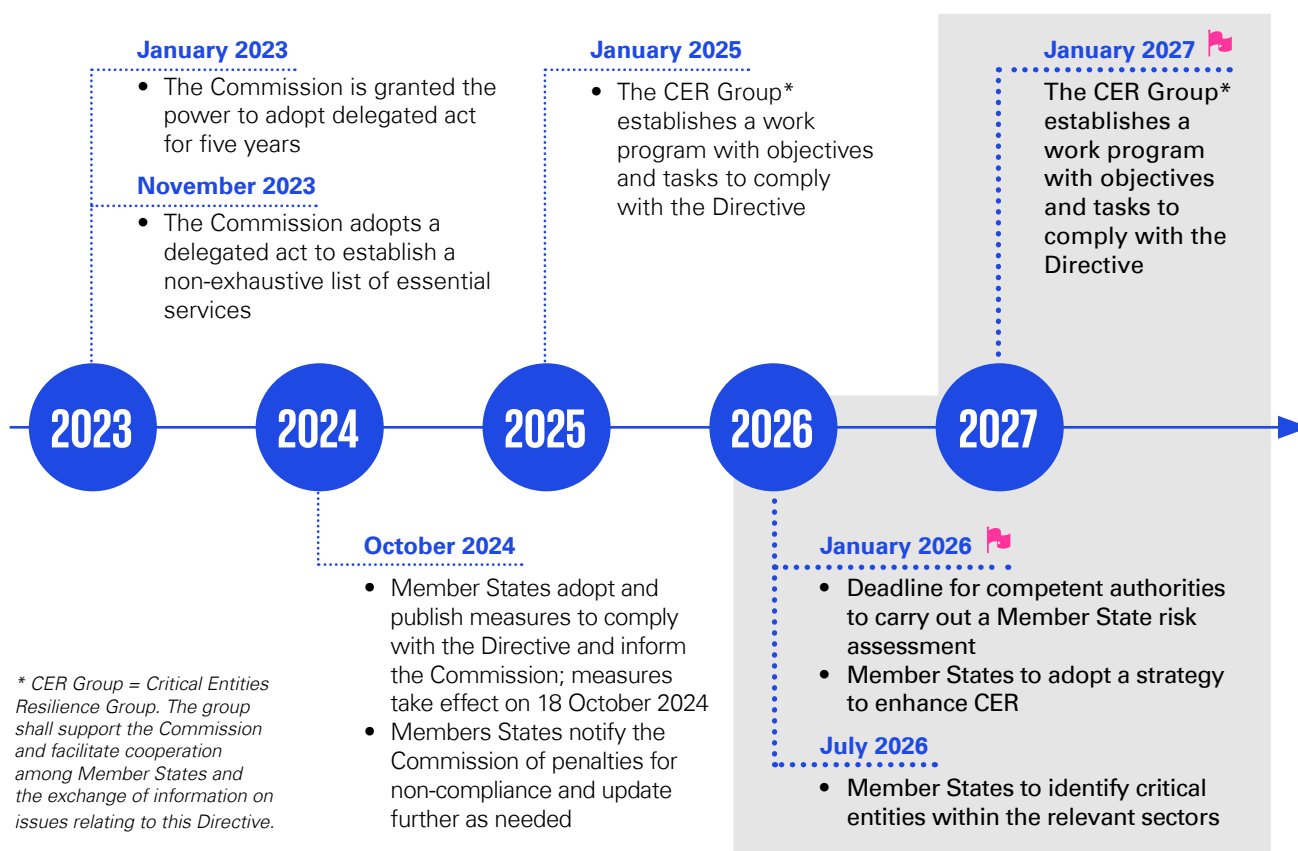
3. Deadlines and implementation timeline

3.1 Milestones for Member States to identify critical entities under the CER

The process of identifying critical entities (CEs) as defined by the CER involves a series of milestones and steps that Member States must undertake to ensure the robust protection and resilience of CIs and essential services. These milestones typically include:

- 1. Baseline assessment:** Member States conduct a baseline assessment of CIs sectors within their jurisdiction to identify key sectors that are vital for societal functioning and economic stability. This assessment serves as the foundation for determining the scope of CEs that fall under the CER.
- 2. Sectorial analysis:** Following the baseline assessment, detailed sectorial analyses are carried out to pinpoint specific entities within critical sectors that provide essential services requiring heightened resilience and protection. These analyses consider criticality, dependence on interconnected systems, and potential impact of disruptions.
- 3. Risk identification and evaluation:** Member States engage in risk identification and evaluation processes to assess the vulnerabilities, threats, and potential consequences that CEs may face. By understanding the risk landscape, authorities can prioritize CEs based on their susceptibility to various threats and the criticality of their services.
- 4. Consultation and validation:** Stakeholder consultation and validation play a crucial role in the identification of CEs, as input from industry experts, regulatory bodies, and relevant stakeholders helps refine the list of entities deemed critical. Collaboration ensures comprehensive coverage and alignment with sector-specific nuances.
- 5. Formal designation:** Once the identification process is complete and consensus is reached, Member States formally designate CEs under the CER, outlining the specific entities that are subject to regulatory requirements for enhancing resilience, security, and continuity of operations.

Deadlines for implementation



3.2 Compliance deadlines for critical entities under the CER

The compliance deadlines for CEs under the CER are structured to allow entities adequate time to implement the necessary measures and safeguards to enhance their resilience posture. Compliance deadlines often follow a phased approach, considering the complexity of operations, resource availability, and the criticality of services provided. Key compliance deadlines typically include:

- 1. Initial compliance assessment:** CEs are required to conduct an initial compliance assessment upon designation to evaluate their existing resilience capabilities, identify gaps, and develop a roadmap for meeting regulatory requirements.
- 2. Implementation of resilience measures:** CEs must implement the prescribed resilience measures and risk management practices within a specified timeline, ensuring the protection of CIs and essential services against a range of threats.
- 3. Testing and validation:** CEs are often mandated to conduct testing, validation, and exercises to validate the effectiveness of their resilience

measures, incident response protocols, and business continuity plans in simulated scenarios.

- 4. Ongoing monitoring and reporting:** Continuous monitoring, evaluation, and reporting of resilience metrics are integral to compliance with the CER. Entities are expected to demonstrate ongoing improvement, adaptability to emerging threats, and transparency in reporting compliance status.
- 5. Periodic review and updates:** Regular reviews and updates of resilience measures, risk assessments, and compliance status are essential for maintaining alignment with evolving threats, regulatory changes, and technological advancements in the CIs landscape.

By adhering to the outlined compliance deadlines and milestones for identifying and safeguarding CEs under the CER, Member States and designated entities can foster a culture of resilience, strengthen their operational resilience, and collectively enhance the security and reliability of CIs and essential services across Europe.

4. Key provisions of the new frameworks for infrastructure resilience

The CER Directive establishes a comprehensive framework to enhance the resilience of CIs in the EU through an all-hazard approach, sector-specific measures, and strict reporting requirements, enabling entities to better prepare for and mitigate potential threats.

As most Member States, including Belgium, are still in the process of working towards transposing the Directive into national law, organizations operating in critical sectors must proactively align their risk management and resilience strategies with the Directive's requirements to ensure compliance and safeguard essential services.

Critical entities risk assessments: The all-hazard approach (Article 12 - Risk assessment by critical entities)

One of the fundamental obligations under the CER Directive is the implementation of a robust risk assessment framework. The Directive mandates that Member States and CEs adopt an **all-hazard approach**, meaning that they must assess and prepare for a broad spectrum of potential threats, including natural disasters, cyber threats, terrorist attacks, and supply chain disruptions, public health emergencies, and hybrid threats. CEs, as defined by the directive and by the separate Member States, must carry out a risk assessment within ten months of receiving the notification referred in Article 6(3), whenever necessary subsequently, and at least every four years. In this risk assessment they should aim to assess all relevant risks that could disrupt the provision of their essential services ("critical entity risk assessment").

CEs are required to:

- Conduct regular risk assessments to identify vulnerabilities and potential disruptions, and report the results and mitigation strategies to national competent authorities. Evaluate interdependencies within and across sectors to understand cascading risks.
- Consider emerging threats such as climate change and geopolitical instability.

Resilience measures for CEs (Article 13).

Article 13 of the CER Directive mandates that Member States ensure critical entities implement proportionate technical, security, and organizational measures to enhance their resilience. These measures include:

- Preventing incidents by taking a comprehensive and holistic approach, including disaster risk reduction and climate adaptation measures.
- Securing infrastructure with adequate physical protection measures.
- Managing crises and ensuring business continuity, particularly by identifying alternative supply chains to facilitate the resumption of essential services.
- Managing employee security, including conducting background checks (as detailed in Article 14) and providing training.

These proportionate measures should then be formalized and regularly updated in a 'resilience plan.' Existing documents with similar content, developed for other purposes and/or for compliance with different legislation, may be used to demonstrate compliance with this directive.

Furthermore, critical entities must develop resilience plans and appoint liaison officers to coordinate and serve as the point of contact with competent authorities.

Enhancing human resource security controls in CEs (Article 14)

Article 14 of the CER Directive outlines the conditions under which CEs may request background checks for individuals in sensitive roles, those with access to secure systems, or potential recruits. These checks must comply with national and EU laws, be proportionate, and aim to assess security risks. They include identity verification and criminal record checks, utilizing the European Criminal Records Information System. Member States must process such requests within a reasonable timeframe, ensuring responses to cross-border criminal record inquiries within 10 working days.

Incidents disrupting or threatening essential services (Article 15)

Article 15 of the CER Directive establishes the obligation for critical entities to promptly notify competent authorities of incidents that significantly disrupt or could disrupt essential services.

Critical entities must inform authorities without undue delay, with an initial notification within 24 hours of becoming aware of an incident and, if necessary, a detailed report within one month. Factors such as the number of affected users, duration, and geographical scope help determine the impact of an incident.

If an incident affects six or more Member States, the competent authorities must notify the European Commission.

Notifications should include all necessary information to assess the incident's nature, cause, and consequences, without exposing the entity to increased liability.

Authorities must share relevant incident details with other affected Member States while ensuring confidentiality and protecting commercial interests. If deemed in the public interest, Member States may choose to inform the public about the incident.

5. How to prepare for the CER Directive?

As the CER Directive is readying to come into full force, organizations have a unique opportunity to take proactive steps to ensure compliance and strengthen their resilience. While enforcement is not immediate, early preparation is key to avoiding disruptions and meeting the requirements outlined in the Directive. At this preparatory stage, it's crucial to identify synergies with ongoing compliance and security projects within your organization. Many initiatives may already be in progress to meet other regulatory requirements or strengthen security: by aligning these existing projects with the CER Directive's objectives, you can ensure a more efficient and cost-effective approach to meeting compliance. This 'by design' and proactive approach not only streamlines your efforts but also anticipates the required changes early, embedding compliance and resilience into the core of your transformation initiatives.

The alignment of the CER Directive with the EU cybersecurity regulatory framework offers a valuable opportunity for entities to develop a comprehensive and integrated resilience strategy to address the complex risks threatening CIs. Leveraging the synergies between these regulations allows organizations to strengthen their defenses, improve response capabilities, and build a culture of resilience that goes beyond individual compliance requirements, ensuring the continuity and reliability of essential services.

Below, we provide a list of CER requirements along with their connections and synergies with other existing European regulations, either in the process of implementation or already enforced. However, it is strongly advised to first verify if the scope of application of these regulations, in terms of processes and assets, is indeed the same.

Requirements and areas of action (CER)	Compliance synergies
Risk assessment (all-hazard approach)	NIS2: Cyber Risk Management DORA: ICT Risk Management Framework Cyber Resilience Act¹: Obligations of Manufacturers GDPR: Data Protection Risks - DPIA AI Act: AI Risk Management
Resilience measures of critical entities (CEs)	NIS2: Cybersecurity Risk Management Measures DORA: Digital Operational Resilience Testing & Managing ICT Third-Party Risk Cyber Resilience Act: Built-in Security GDPR: Data Security Measures AI Act: AI Resilience & Security
Article 14: Enhancing Human Resource Security Controls in Critical Entities	NIS2: Human resources security measures GDPR: Employees' background checks
Article 15: Incidents Disrupting or Threatening Essentials Services	DORA: ICT-Related Incident Reporting NIS2: Cyber Risk Management Cyber Resilience Act: Incident Reporting GDPR: Data Breach Notification AI Act: AI Monitoring & Reporting

¹ The Regulation, as per Article 2, applies to products with digital elements made available on the market, the intended purpose or reasonably foreseeable use of which includes a direct or indirect logical or physical data connection to a device or network.

6. Next steps to strengthen your organization

1. Understanding whether your organization qualifies as a critical entity:

Determine if your organization falls under the scope of the CER Directive based on its sector and the potential consequences of service disruptions. Understanding your designation as a critical entity is key to ensuring compliance. (Refer to Directive (EU) [2022] OJ L333/164, Articles 6 and 171.)

2. Understand the requirements of the CER Directive:

Gain a clear understanding of the Directive's obligations, including **risk assessments, resilience planning, incident reporting, and mitigation strategies**. These elements are fundamental to enhancing your organization's resilience against disruptions.

3. Strengthen and modernize your resilience strategy:

- Evaluate and mitigate risks: Perform comprehensive risk assessments to identify threats, their potential impacts, and how they align with your organization's risk tolerance. (Article 122)
- Enhance governance and resilience structures: Review and refine your governance framework to support an integrated, data-driven resilience model. Leverage technology, such as automation and analytics, to strengthen risk management.
- Prioritize critical services and functions: Identify key business services and their dependencies, ensuring

resilience efforts focus on protecting what is most essential for your operations and customers. Align business continuity, cybersecurity, IT disaster recovery, and supply chain security to maintain operational stability. (Article 133)

- Improve crisis management capabilities: Update incident response plans to enable swift containment and resolution of disruptions. Ensure compliance with the 24-hour notification requirement and establish a robust communication strategy to manage stakeholders effectively. (Articles 13 and 154)
 - Conduct Ongoing Training and Simulations: Develop a structured training and testing program for crisis response, using realistic scenarios to assess preparedness and response effectiveness. Leverage real-time data to evaluate and enhance resilience strategies. (Article 135)
- ## 4. Stay informed on CER Directive updates:
- Keep track of regulatory changes and deadlines to maintain compliance and adapt to evolving requirements. Even if your organization is not directly classified as a critical entity, assess whether you serve as a supplier to one, as this may still require adherence to the Directive's provisions.

This approach ensures your organization is well-prepared to comply with the CER Directive and effectively manage resilience challenges.

6.1 KPMG expertise and opportunities for support

KPMG's expertise and support services offer a comprehensive and integrated approach to regulatory compliance and resilience, enabling organizations to address multiple EU regulations in a coordinated and strategic way. Rather than treating each regulation in isolation, we have structured the service line around the four key areas of action as derived by the Directive:

1. Risk Assessment

- Compliance and regulations: Regulatory scoping and assessment
- Resilience maturity assessment
- Risk quantification: Comprehensive risk assessment (All-Hazard Approach)
- Third-party risk management (TPRM)

2. (Operational) Resilience

- Integrated governance and ICT framework
- Business continuity management support
- Technology contingency
- Disaster recovery testing
- Crisis response and communications plan
- Crisis management exercising (tabletop exercises)
- OT – VR tabletop







3. Enhancing human resource security controls

- Governance and strategy for the introduction of specific controls over the employee (information protection throughout the entire life cycle)
- Baseline response training
- BoD and senior management training

4. Incident management

- Managed detection and response
- Security intelligence services
- Simulation of advanced attacks: Red/Purple teaming, Gold teaming
- BCP/Playbook Testing
- Incident response and communication plans
- Incident root cause analysis and post-incident reviews

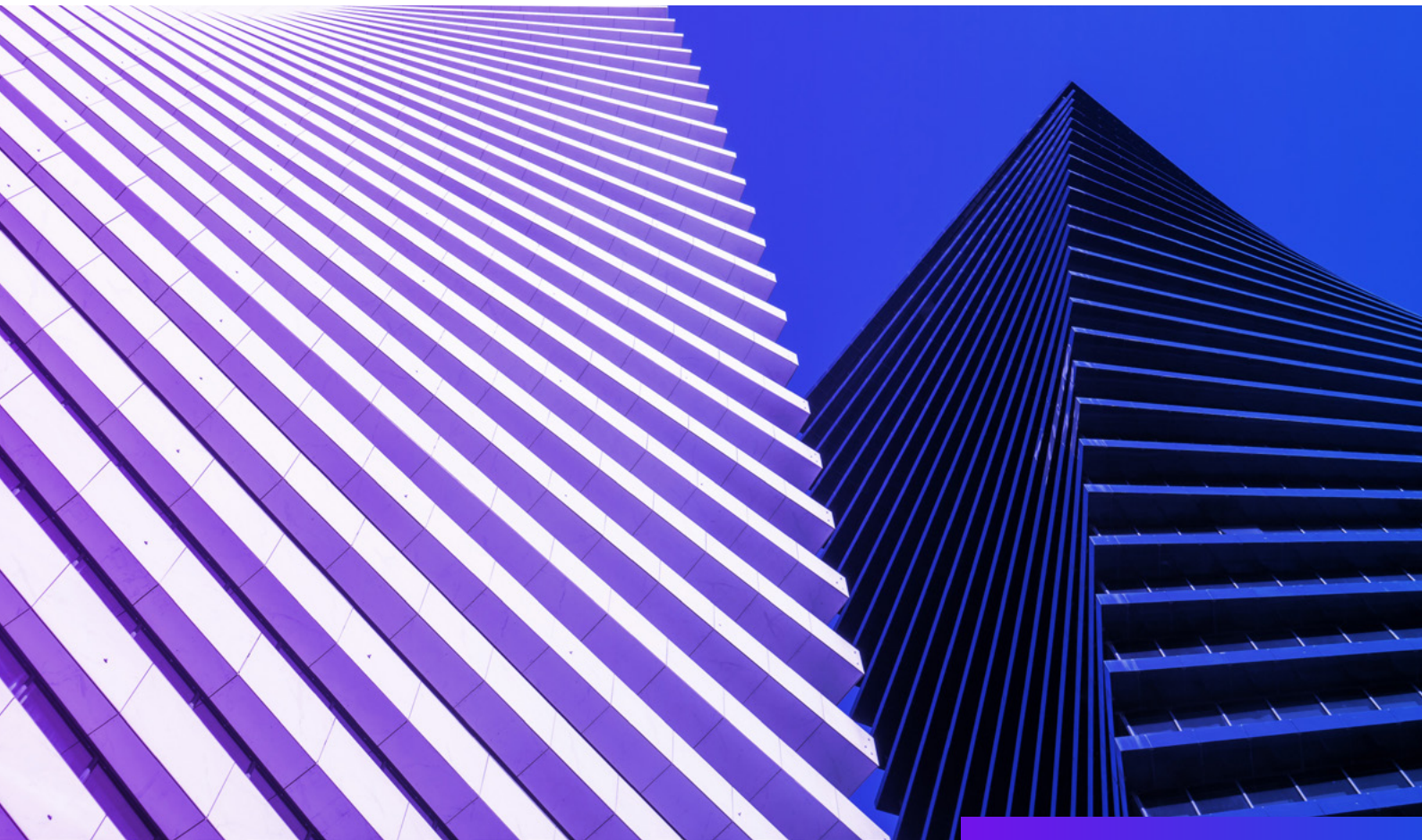
The four key areas reflect the core pillars of resilience across DORA, NIS2, the Cyber Resilience Act, the CER Directive, GDPR, and the AI Act. Each activity has been carefully mapped to one or more regulations, ensuring that compliance efforts are streamlined, non-duplicative, and cross-functional.

CER 	DORA 	NIS2 	CRA 	AI Act 	GDPR 
Risk Assessment & Management	ICT Risk Management (Article 6)	Cyber Risk Management (Article 14)	Obligations of Manufacturers (Article 13)	AI Risk Management (Article 9)	Data Protection Risk Assessment - DPIA (Article 35)
KPMG services	<ul style="list-style-type: none">Regulatory scoping analysis & gap analysisResilience Maturity Assessment			<ul style="list-style-type: none">Comprehensive Risk Assessment (all-hazard approach)ICT Third-Party Risk Management (TPRM)	
Resilience Measures	Digital Operational Resilience Testing (Article 24)	Cybersecurity Measures (Article 21)	Built-in Security (Article 7)	AI Resilience & Security (Article 15)	Data Security Measures (Article 32)
KPMG services	<ul style="list-style-type: none">Integrated Governance ICT FrameworkDisaster Recovery TestingBusiness Impact Analysis			<ul style="list-style-type: none">Business Continuity Management SupportCrisis Response & Communication Plans	
Human Resources Security Controls	Human Resources Security Measures (Article 21)				Access Control Measures (Article 88)
KPMG services	<ul style="list-style-type: none">Baseline Response TrainingBoD & Senior ManagementGold Teaming			<ul style="list-style-type: none">Tabletop ExerciseBCP/Playbook TestingOT-VR Tabletop	
Incidents management	ICT Related Incident Reporting (Article 17)	Incident Reporting (Article 23)	Incident Reporting (Articles 14 - 17)	AI Monitoring & Reporting (Article 73 & Chapter IX)	Breach Notification (Articles 33 & 34)
KPMG services	<ul style="list-style-type: none">Incident Root Cause Analysis & Post-Incident ReviewsComms Testing			<ul style="list-style-type: none">Crisis Management ExerciseIncident Response & Communication Plans	

7. Conclusion

As organizations prepare for the full enforcement of the CER, the next step is to actively engage with the Directive's requirements and take a proactive approach to compliance. This means reviewing and aligning current risk management, business continuity, and security practices with the CER's provisions. Entities should consider collaborating with experts in risk management, cybersecurity, business continuity and compliance to ensure all aspects of the Directive are effectively addressed. By doing so, organizations not only secure compliance but also build long-term resilience, positioning themselves to manage both current and future risks with confidence. Starting early will lead to smoother implementation, reduce operational disruption, and help mitigate any potential gaps in resilience.

The path is clear: plan ahead, consult with experts, and take decisive action now to stay ahead of the regulatory curve and ensure your organization is fully prepared for the future. By starting early and integrating the Directive's requirements with your ongoing projects, you can better manage risks, protect critical services, and align your operations with the Directive's goals, ensuring full readiness when the regulations come into effect and when a disruptive event occurs.



Annex

Mapping of CER Requirements vs. Other EU Cybersecurity Regulations

Requirements and areas of action (CER)	Compliance synergies with the EU Cyber regulatory framework
Article 12: Risk-Assessment by critical entities: It requires to adopt an all-hazards approach, focusing on the resilience of both network and information systems, as well as their physical components and environment. Critical entities must implement a comprehensive risk assessment framework addressing all types of hazards, whether natural, man-made, accidental, or intentional (including natural disasters, cyber threats, terrorist attacks, and supply chain disruptions). Where a critical entity has carried out other risk assessments or drawn up documents pursuant to obligations laid down in other legal acts that are relevant for its critical entity risk assessment, it may use those assessments and documents to meet the requirements set out in this Article.	NIS2 Cyber Risk Management: Requires assessing and manage cybersecurity risks to their networks and systems, aligning with the need for an all-hazard approach. Ref.: Article 14, Recitals 77, Recitals 90-91.
	DORA ICT Risk Management Framework: <ul style="list-style-type: none">• Focuses on ICT risk management in financial services, assess and manage risks to their digital operations, including cybersecurity risks, to ensure business continuity in the event of disruptions.• Entities must establish a comprehensive ICT risk management framework, that identifies, assesses, and mitigates ICT risks. This framework should include strategies, policies, and procedures to protect all information and ICT assets, such as software, hardware, and data centers. Ref.: Chapter II: ICT Risk Management – Article 6 and 7
	Cyber Resilience Act² (potentially limited to Digital Infrastructure and Health providers as defined by CER) Obligations of Manufacturers: Manufacturers of products with digital elements must assess and mitigate cybersecurity risks to prevent vulnerabilities and disruptions to services and products. Ref.: Article 13, Recital 37.
	GDPR Data Protection Risks - DPIA: GDPR focuses on data protection and directly addresses risk management for personal data breaches by emphasizing the assessment of risks to individuals' rights and freedoms. Ensuring effective data protection risk management, tailored to the sector of critical entities, is essential for full compliance with CER requirements. Ref: Article 35, Recital
	AI Act AI Risk Management: Requires the implementation of a comprehensive risk management system for AI systems, ensuring that high-risk AI applications used in critical sectors are resilient to potential disruptions, including those arising from cyber threats. Ref.: Article 9, Recital 66

² The Regulation, as per Article 2, applies to products with digital elements made available on the market, the intended purpose or reasonably foreseeable use of which includes a direct or indirect logical or physical data connection to a device or network.

Requirements and areas of action (CER)

Article 13: Resilience Measures of critical

entities: Take appropriate and proportionate technical, security and organizational measures to ensure their resilience, including measures necessary to:

- Prevent Incidents: Implement disaster risk reduction and climate adaptation strategies to avert potential disruptions
- Ensure Physical Protection
- Respond to, Mitigate, Recover from Incidents
- Manage Employee Security
- Raise Awareness Among Personnel
- Develop a Resilience Plan
- Appoint a Liaison Officer

Compliance synergies with the EU Cyber regulatory framework

DORA

- **Digital Operational Resilience Testing:** Regular testing of digital operational resilience is mandated to ensure the effectiveness of implemented strategies and systems. **Ref:** Chapter IV: Digital operational resilience testing -Article 24, Recital 56
- **Managing ICT Third-Party Risk:** Entities must manage risks associated with ICT third-party service providers, including conducting due diligence and monitoring their performance. **Ref:** Chapter V: Managing of ICT Third-Party Risk - Article 28-31, Recital 31,56

NIS2

Cybersecurity Risk Management Measures:

mandates that entities implement appropriate and proportionate technical, operational, and organizational measures to manage risks to the security of their network and information systems. The measures should be based on an all-hazards approach and include at least the following:

- Risk Analysis and Information System Security Policies, Incident Handling,
- Business Continuity and Crisis Management,
- Supply Chain Security,
- Security in Network and Information Systems Acquisition, Development, and Maintenance,
- Policies and Procedures to Assess the Effectiveness of Cybersecurity Risk-Management Measures,
- Basic Cyber Hygiene Practices and Cybersecurity Training, Use of Cryptography and Encryption,
- Human Resources Security (related to access and asset management)
- Use of Multi-Factor Authentication or Continuous Authentication Solutions

Ref: Chapter IV, Article 21, Recitals 44-47-48

In Belgium, as mandated by the Centre for Cybersecurity Belgium (CCB), organizations are required to adhere to specific key measures and implement the CyberFundamentals (CyFun) framework corresponding to their designated assurance level. The CyFun framework offers four assurance levels, Small, Basic, Important, and Essential, each tailored to the organization's size, risk exposure, and sector-specific requirements. These levels guide organizations in implementing appropriate cybersecurity measures to enhance their resilience against cyber threats.

Cyber Resilience Act (limited to Digital Infrastructure and Health providers as defined by CER)

Built-in Security: Enforces that products with digital elements have built-in security features and resilience measures, ensuring that any disruption or vulnerability can be quickly identified and addressed. **Ref.:** Article 7, Recital 22

GDPR

Data Security Measures: Resilience measures under GDPR focus on the security of personal data, requiring entities to ensure the availability and integrity of data through appropriate technical and organizational measures. **Ref.:** Article 32

AI Act

AI Resilience & Security: Requires that AI systems be designed to ensure their resilience, with particular focus on high-risk applications in critical sectors, ensuring accuracy, robustness, and secure deployment under normal and crisis conditions. **Ref.:** Article 15, Recital 75, Recital 76

Requirements and areas of action (CER)

Article 14: Enhancing Human Resource Security Controls in Critical Entities: addresses background checks for critical entity personnel in sensitive roles. Checks must be lawful, proportionate, and timely, involving identity verification and criminal record assessments through the EU system, with cross-border inquiries answered within 10 days.

Article 15: Incidents Disrupting or Threatening Essentials Services: promptly notify authorities of disruptive incidents, with initial notification within 24 hours and detailed reports within a month. Factors like affected users and duration determine impact assessment. Information sharing among authorities and possible public disclosure can occur in the public interest.

Compliance synergies with the EU Cyber regulatory framework

NIS2

Human resources security measures: According to Article 21, risk management measures can also relate to or be applied to human resources. Therefore, in compliance with a risk-based approach, personnel background check measures can be applied if deemed proportionate. **Ref.:** *Article 21, Article 28*

GDPR: Data protection requirements must be considered and implemented if background checks are conducted. For instance, employers may only perform criminal record checks if permitted by law and in compliance with national or EU regulations. **Ref.:** *Article 9, Article 10*

DORA

ICT-Related Incident Reporting: Establishes obligations for financial entities to implement a management process for monitoring and logging ICT-related incidents. Incidents are classified based on criteria specified by relevant supervisory authorities, ensuring a standardized approach to incident handling. **Ref.:** *Chapter III: ICT-related incident management process - Article 17, Recital 24*

NIS2

Incident Reporting, Network and Information Systems: Requires essential entities to report and notify in case of incident. It defines what constitutes an incident, the mandatory reports, and the content required in these reports. **Ref.:** *Article 23, Chapter IV, Recitals 101, 105*

Cyber Resilience Act (limited to Digital Infrastructure and Health providers as defined by CER)

Incident Reporting: Requires the reporting of significant cybersecurity incidents related to products with digital elements, aiming to prevent the propagation of security vulnerabilities and ensuring timely remediation. **Ref. :** *Article 14, Article 15, Article 16, Article 17, Recital 28*

GDPR

Data Breach Notification: Obliges organizations to notify data breaches involving personal data, ensuring that individuals' rights are protected, and services can recover quickly following a disruption. **Ref.:** *Article 33, Article 34, Recital 85*

AI Act.

AI Monitoring & Reporting: It mandates that high-risk AI systems undergo continuous post-market monitoring to proactively detect potential issues. It also requires the reporting of serious incidents that may disrupt critical services. This ensures transparency regarding AI failures that could pose risks to public safety or business continuity. **Ref.:** *Article 3(49), Article 73, Recital 71, Chapter IX- Post-market monitoring, information sharing and market surveillance*

Area of Action: 1. Risk Assessment and Management

KPMG expertise and opportunity for support

Regulatory Scoping & Assessment: Identifies applicable regulations and breaks them down into specific obligations, assessing the current compliance status to prioritize actions. The main goal is to optimize efforts by addressing overlaps across requirements.

Resilience Maturity Assessment (RMA): Evaluates current resilience capabilities and maturity across systems, people, and processes.

Comprehensive Risk Assessment (All-Hazard Approach): Identifies and assesses risks (ICT, OT, data, AI, cybersecurity, operational) across critical services, systems, and partners to prioritize mitigation efforts. This activity is essential across all regulations, laying the foundation for compliance by highlighting risks that require focused attention, mitigation, or monitoring.

ICT Third-Party Risk Management (TPRM): Assesses risks from external providers to align contracts with risk levels, in line with the overall enterprise risk assessment. Ensures third-party resilience and security meet regulatory expectations

Area of Action: 2. (Operational) Resilience

KPMG services and opportunity for support

- **Integrated Governance and ICT Framework:** Designs a sustainable governance model with clearly defined roles and responsibilities. Develops comprehensive policies aligned with multiple regulations to streamline compliance and reduce conflicts, ensuring consistent and efficient regulatory management.
- **Business Continuity Management Support:** Advisory support to build and manage a Business Continuity Management System (BCMS). Covers Business Impact Analysis development and execution, risk assessment, planning, testing, and compliance with continuity standards, to ensure operational continuity during and after disruptions. KPMG provides furthermore audits support to assess BCMS effectiveness based on ISO 22301.
- **Technology Contingency Plans** Develops, implements, and tests plans to maintain or restore critical operations. Draws on Risk Assessment to ensure readiness for disruptions while supporting compliance with DORA, NIS2, AI Act, and CER Directive.
- **Disaster Recovery Testing:** Verifies recovery of critical systems and data from backup sources and tests IT recovery procedures to validate system and data restoration
- **Crisis Response & Communications Plan:** Designs and tests structured crisis and communication plans.
- **OT – VR Tabletop:** Virtual Reality-based simulations for OT environments and CIs. Trains teams in safe, immersive scenarios without impacting real systems
- **Tabletop Exercise:** Discussion-based simulation for decision-makers to practice incident response. Improves preparedness, communication, and decision-making without real disruptions.



Area of Action: 3. Enhancing Human Resource Security Controls

KPMG expertise and opportunity for support

- **Governance and strategy for the introduction of specific controls over the employee:** To develop a strategy for increasing controls over personnel while ensuring compliance with data protection and privacy laws
- **Baseline Response Training:** Establishing fundamental security awareness and response training programs to ensure personnel understand their roles in maintaining compliance with CER/ NIS2. This includes training on lawful and proportionate background check requirements and handling sensitive personnel data securely.
- **BoD and senior management:** Awareness and training program on ICT risk management and Digital Operation Resilience.

Area of Action: 4. Incidents management

KPMG expertise and opportunity for support

- **Managed detection and response:** security monitoring, and threat vulnerability management service with the aim to enhance an organization's ability to detect, respond to, and recover from security incidents effectively.
- **Security Intelligence Services:** Delivers advanced threat detection through Threat Hunting, Attack Surface Monitoring, and Surveillance. Provides strategic insights with tailored intel and real-time intelligence feeds.
- **Red / Purple Teaming:** Red Team simulates real attacks; Purple Team fosters collaboration with defense teams. Enhances detection, response, and overall cyber resilience.
- **Gold Teaming:** Advisory service focused on executive crisis response and governance. Evaluates leadership's alignment with strategic priorities during incidents.
- **Incident Response & Communication Plans:** Develops and tests structured response and communication plans for disruptive events.
- **Incident Root Cause Analysis & Post-Incident Reviews:** Investigates incident causes and conducts structured post-incident reviews. Ensures lessons learned are fed into compliance and improvement efforts to enhance future resilience.
- **BCP / Playbook Testing:** Tests business continuity plans and incident response playbooks in simulated events.



Contact



Olivier Elst
**Partner, Risk & Regulatory
Advisory**
KPMG in Belgium

M: +32 (0)485 17 83 48
E: oelst@kpmg.com



Benny Bogaerts
**Partner, Technology
Advisory**
KPMG in Belgium

M: +32 (0) 477 30 14 49
E: bbogaerts@kpmg.com



Stella Tsatsaki
**Senior Manager, Risk & Regulatory
Advisory**
KPMG in Belgium

M: +32 (0)499 94 52 77
E: stsatsaki@kpmg.com



Martina Castiglioni
**Manager, Risk & Regulatory
Advisory**
KPMG in Belgium

M: +32 (0)479 85 01 62
E: mcastiglioni@kpmg.com

kpmg.com/be



De in dit document opgenomen informatie is van algemene aard en heeft niet tot doel de specifieke omstandigheden van een bepaalde persoon of entiteit te behandelen. Wij streven ernaar juiste en tijdige informatie te verstrekken. Wij kunnen echter geen garantie geven dat dergelijke informatie op de datum waarop zij wordt ontvangen nog juist is of in de toekomst correct zal blijven. Daarom adviseren wij u geen beslissingen te nemen op grond van deze informatie tenzij na het inwinnen van advies van deskundigen na een grondig onderzoek van de desbetreffende situatie.

© 2025 KPMG Advisory, a Belgian BV/SRL and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.