



Critical Entities Resilience Directive Deloitte Cyber Regulatory Compliance

A directive that aims to **reducing vulnerabilities and strengthening the resilience of critical entities** against various threats. Key focus areas include:



Enhancing resilience against various threats, including cyberattacks, natural disasters, and terrorist activities.



Protecting digital service users by fostering trust, minimizing exposure to illegal, harmful, or manipulative content.



Ensuring transparency and oversight, with specific regulatory requirements for monitoring digital service providers.

WHO DOES CER APPLY TO?

EU Member States have to **identify “critical entities” essential for maintaining the continuity of societal and economic functions in the EU by July 2026**. The identified entities have to carry out **risk assessments** and adopt **resilience-enhancing measures** to prevent, respond to, and mitigate incidents disrupting the provision of their services. The following **sectors** are impacted:



BANKING



**FINANCIAL MARKET
INFRASTRUCTURE**



**DIGITAL
INFRASTRUCTURE**



TRANSPORT



ENERGY



HEALTH



DRINKING WATER



WASTEWATER



**PUBLIC
ADMINISTRATION**



SPACE



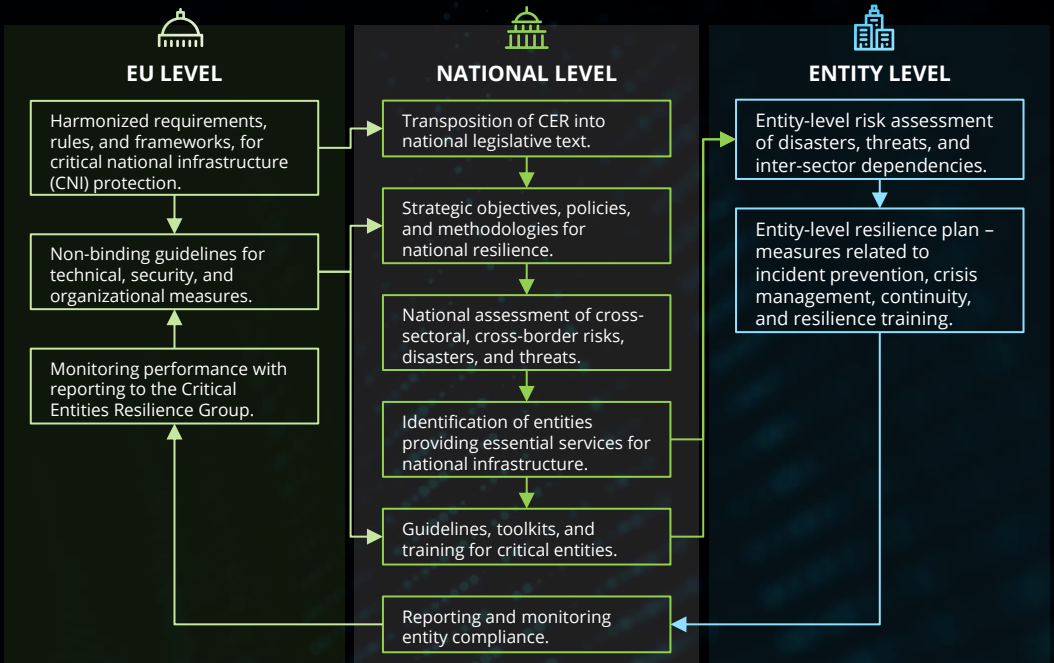
FOODS

The CER directive provisions must be transposed into **national laws**. In the Czech Republic, it is implemented through the **Critical Infrastructure Act**.

HIGH-LEVEL COMPARISON WITH DORA & NIS2

	CER Directive	NIS2 Directive	DORA Regulation
Affected sectors	<ul style="list-style-type: none"> Banking Financial Market Infrastructure Digital Infrastructure Transport Energy Health Drinking Water Waste Water Public Administration Space Food Production, Processing, & Distribution 	<p>High Criticality Sectors:</p> <ul style="list-style-type: none"> Banking Financial Market Infrastructure Digital Infrastructure Transport Energy Health Drinking Water Waste Water Public Administration ICT Service Management Space <p>Other Critical Sectors:</p> <ul style="list-style-type: none"> Postal & Courier Services Waste Management Production, Processing & Distribution of Food Manufacturing, Production & Distribution of Chemicals Manufacturing Research Digital Providers 	<p>Financial Sector – Banks, Insurance Companies, Investment Firms, Payment Providers, and Other Financial Entities, as well as ICT third-party service providers</p>
Primary focus	All-hazards resilience in specific “critical” sectors	Cyber risk management with a specific focus on network and information systems	Digital operational resilience with a specific focus on ICT risk management, incident reporting & third-party risk management
Risk focus	Various risk types, including natural and man-made risks	Cyber-related risks	ICT & cyber risks

PATH TO MORE RESILIENT EUROPE



HOW CAN DELOITTE HELP?

Our **team of experts** delivers a full suite of services tailored to the needs of each Client, ranging from **initial gap assessments** to strategic **guidance** and hands-on **implementation support**.



**APPLICABILITY
ASSESSMENT &
RISK ANALYSIS**



**GAP ANALYSIS &
REMEDATION**



**IMPLEMENTATION
& COMPLIANCE
SUPPORT**



**TRAINING &
RESILIENCE-
BUILDING
WORKSHOPS**

CONTACT US



Ratko Drca, Director
rdrca@deloittece.com



Donika Dimov, Senior Manager
dodimov@deloittece.com