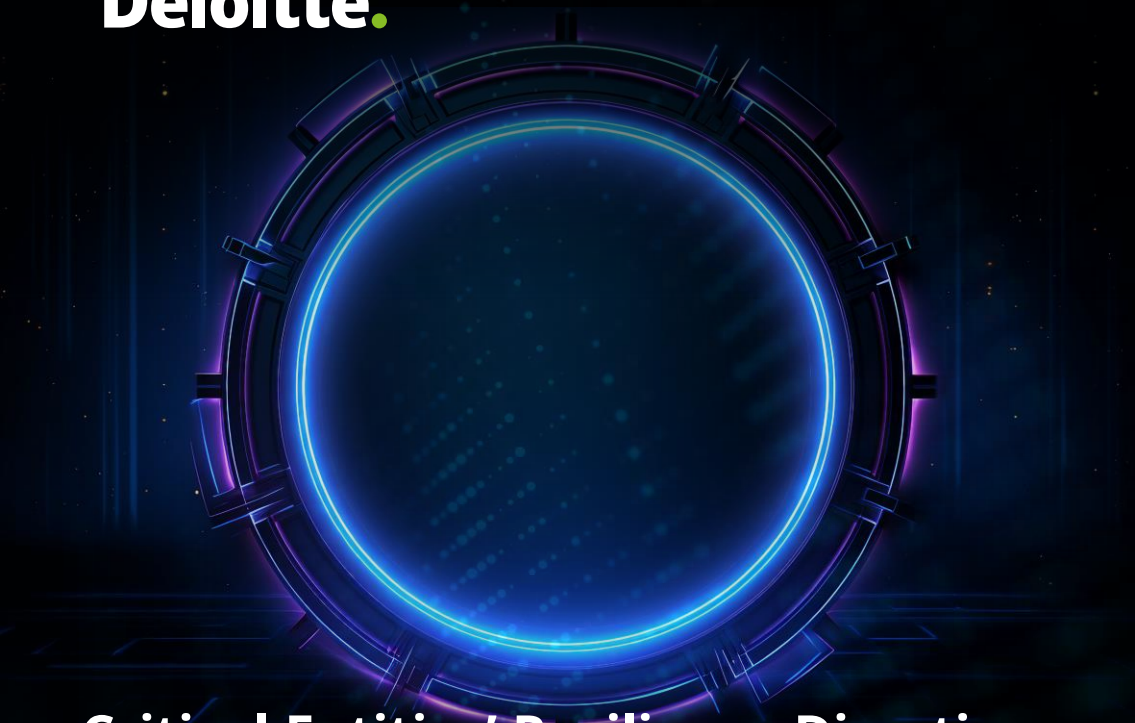
Deloitte.



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?

Deloitte.

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**.

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 & REMEDIATION**
- **IMPLEMENTATION & COMPLIANCE SUPPORT**
- **TRAINING & RESILIENCE-BUILDING WORKSHOPS**

CONTACT US

Jakub Höll, Director
jholl@deloittece.com

Martin Antoš, Manager
mantos@deloittece.com

HIGH-LEVEL COMPARISON

Deloitte.

	CER Directive	NIS2 Directive	DORA Regulation
Affected sectors	– Banking – Financial Market Infrastructure – Digital Infrastructure – Transport – Energy – Health – Drinking Water – Waste Water – Public Administration – Space – Food Production, Processing, & Distribution	***High Criticality Sectors:*** – Banking – Financial Market Infrastructure – Digital Infrastructure – Transport – Energy – Health – Drinking Water – Waste Water – Public Administration – ICT Service Management – Space ***Other Critical Sectors:*** – Postal & Courier Services – Waste Management – Production, Processing & Distribution of Food – Manufacturing, Production & Distribution of Chemicals – Manufacturing – Research – Digital Providers	Financial Sector – Banks, Insurance Companies, Investment Firms, Payment Providers, and Other Financial Entities, as well as ICT third-party service providers
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