

Statement

European Commission guidance on the Cyber Resilience Act

Brussels, 13 October 2026

The **Cyber Resilience Act**¹ (CRA) establishes horizontal cybersecurity requirements **for products with digital elements** (PDEs) made available on the Union market. Its main obligations will apply from 11 December 2027 to almost all economic sectors in the European market. From that date, manufacturers placing PDEs on the market must ensure that those products meet the applicable essential cybersecurity requirements, complete the relevant conformity assessment and provide vulnerability support throughout the support period.

The railway sector is characterised by interconnected systems with service lives often exceeding 20 years and governed by harmonised interoperability requirements, with upgrades and extensions needing to maintain compatibility with the existing network or allow for a gradual transition. This poses an undeniable additional challenge for the railway sector in implementing the CRA.

On 27 July 2026, the European Commission published its [guidance on the application of the CRA](#)². EIM welcomes this practical guidance. Although it is non-binding, it provides an important common reference for the consistent implementation of the CRA and gives economic operators greater legal and operational clarity. EIM is particularly pleased that the Commission's interpretation confirms many of the interpretations regarding the specifics of the railway sector that EIM has had since the adoption of the CRA:

1) The spare parts exemption applies to genuinely identical replacements

Article 2(6) of the CRA excludes spare parts from its scope where they are supplied to repair or extend the durability of a product already placed on the market and replace an identical component manufactured according to the same specifications. EIM welcomes the Commission's confirmation that this exemption is limited to genuine replacements. A component with different cybersecurity characteristics cannot be treated as an exempt spare part merely because it performs the same function or has been

¹ Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act), ELI: <http://data.europa.eu/eli/reg/2024/2847/oj>.

² European Commission, Commission guidance on the application of the Cyber Resilience Act (CRA), C(2026) 5252 final, 27 July 2026.

configured to match the original. It must instead be assessed as a PDE in its own right, including any risks arising from its integration into the existing product.³

However, while EIM recognises why the Commission interprets “identical” with reference to characteristics relevant to cybersecurity as requiring every feature of a replacement to be unchanged could lead to unreasonable results, **Article 2(6), however does not expressly contain that qualification.**⁴ Without clearer criteria for determining which differences are permissible, the interpretation could broaden the exemption beyond genuinely identical spare parts and allow it to be used to circumvent CRA obligations. **EIM therefore calls for this concept to be better defined and applied narrowly, including in cases such as Example 38 in the guidance.**

2) The CRA applies to the product placed on the market, taking account of its system context

Railway projects are often developed as systems comprising many interdependent products. Under the CRA, the manufacturer’s obligations attach to the PDE placed on the market. This may be a separately supplied component or a complex system supplied as a single PDE.⁵ The manufacturer must therefore identify the relevant PDE(s) and assess its cybersecurity risks at that level, including where it is supplied as part of a wider railway project.⁶

EIM welcomes the Commission’s confirmation that the CRA can accommodate the realities of rail. The manufacturer should take account of a PDE’s intended use, operating environment and interactions with other systems when assessing its risks. This allows the assessment to reflect its place in the wider railway system while maintaining the manufacturer’s responsibility for the product it supplies. The Commission also makes clear that manufacturers must keep the risk assessment under review during the support period and reassess constraints arising from existing systems. Where those constraints can be lifted or reduced over time, the manufacturer should update the PDE accordingly, confirming EIM’s position that the CRA is here to gradually improve the cybersecurity level of the sector.⁷

3) Pre-existing designs and interoperability constraints do not remove CRA obligations

The Commission recognises that complex systems may have long development cycles and rely on contracts, architectures or interoperability standards established before the CRA applies. Those circumstances do not exclude a PDE from the CRA if it is placed on the market after 11 December 2027.⁸ EIM has held that a pre-existing design does not automatically require redesign and that a pre-existing design or contract cannot justify placing a non-compliant PDE on the market. It therefore welcomes the Commission’s clarification that compliance does not necessarily require redesign: existing security measures may suffice where a cybersecurity risk assessment demonstrates that the PDE meets the applicable essential requirements.

The Commission also explains how this approach accommodates interoperability with existing systems. Where a PDE needs to communicate using an older, less secure protocol, the manufacturer may support that protocol where necessary, provided it assesses and mitigates the associated risks. Where technically feasible, the PDE is also expected to support a secure protocol and use it by default; the older protocol should be used only where interoperability requires it.⁹

³ §§ 97, 98 and 101 *ibid.*

⁴ §§ 99—100 *ibid.*

⁵ § 29 *ibid.*

⁶ § 156 *ibid.*

⁷ § 32 *ibid.*

⁸ § 30 *ibid.*

⁹ § 32 and Example 10 *ibid.*

4) Responsibility for CRA compliance remains with the manufacturer

Railway infrastructure managers and other operators must manage risks to their networks and information systems under the NIS2 Directive, including risks arising from the products they procure.¹⁰ The CRA complements these duties by requiring manufacturers to assess the cybersecurity risks of the PDEs they place on the market and demonstrate compliance with the applicable essential requirements. An operator's responsibility for its network does not transfer the manufacturer's product obligations to the customer. The Commission confirms that neither an agreement with the customer nor considerations of cost or commercial feasibility justify leaving product risks unaddressed.¹¹

EIM further considers that manufacturers should avoid defining a PDE's intended purpose more narrowly than its foreseeable uses require. Even where a PDE is tailored to one customer's operating environment, it should later be able to be transferred or reused elsewhere. Manufacturers should therefore design for a sufficiently broad intended use where feasible, document any necessary limits clearly, and reserve interoperability related constraints for circumstances where they are genuinely needed.

Conclusion

EIM welcomes the European Commission's CRA practical guidance and the clarity it provides for complex, long-lived and interoperable products. EIM is pleased that the Commission's interpretation aligns with EIM's position on the scope of the spare-parts exemption, the need to apply the CRA at the level of the relevant PDE, the treatment of products designed or contracted before the CRA applies, and the manufacturer's responsibility for product compliance.

These clarifications support legal certainty and a more consistent allocation of responsibilities throughout the rail supply chain. They should now be fully reflected by the sector and in the practical implementation of the CRA.

About EIM

EIM, the association of European Rail Infrastructure Managers, was established in 2002 to promote the interests and views of the independent infrastructure managers in Europe, following the liberalisation of the EU railway market. It also provides technical expertise to the appropriate European bodies such as the European Railway Agency. EIM's primary goal is promoting growth of rail traffic and the development of an open sustainable, efficient, customer orientated rail network in Europe. For further info, please consult www.eimrail.org

This EIM document is intended for public information purposes. While every effort has been made to ensure the accuracy of its contents, EIM assumes no responsibility for information sourced from third parties, technical inaccuracies, typographical errors, or other discrepancies. Information and links are subject to change without notice.

¹⁰ Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive), ELI: <http://data.europa.eu/eli/dir/2022/2555/oj>, Art. 21(2)(d) and (e).

¹¹ §§ 31–32 and 156–163 of the Commission CRA guidance.