German Banking Industry Committee

Die Deutsche Kreditwirtschaft

Comments

Draft Communication on Commission guidance on the application of the Cyber Resilience Act (CRA)

Lobby Register No R001459
EU Transparency Register No 52646912360-95

Contact:
Berit Schimm
Telephone: +49 30 2021-2100
Telefax: +49 30 2021-1900
E-mail: b.schimm@bvr.de

Berlin, 1 April 2026

The **German Banking Industry Committee** is the joint committee operated by the central associations of the German banking industry. These associations are the Bundesverband der Deutschen Volksbanken und Raiffeisenbanken (BVR), for the cooperative banks, the Bundesverband deutscher Banken (BdB), for the private commercial banks, the Bundesverband Öffentlicher Banken Deutschlands (VÖB), for the public-sector banks, the Deutscher Sparkassen- und Giroverband (DSGV), for the savings banks finance group, and the Verband deutscher Pfandbriefbanken (vdp), for the Pfandbrief banks.

Coordinator:
National Association of German Cooperative Banks
Schellingstraße 4 | 10785 Berlin | Germany
Telephone: +49 30 2021-0
Telefax: +49 30 2021-1900
https://die-dk.de/

Lobby Register No R001459
EU Transparency Register No 52646912360-95

Comments „Draft Communication on Commission guidance on the application of the CRA"

The German Banking Industry Committee fully recognizes that the Cyber Resilience Act will enhance cybersecurity standards of products that contain a digital component, requiring manufacturers and retailers to ensure cybersecurity throughout the lifecycle of their products from 2027 onward. The Commission guidance can help better understand the CRA requirements. In this context, there are still a number of questions, which we explain in the attached appendix.

The purpose of the Guidance chapter 1.2 no. 9 mentions that in line with Article 26 of the CRA, the Commission may consider issuing further guidance, including guidance targeted at manufacturers subject to the CRA and other Union harmonisation legislation or to other related Union legal acts. We support the issuance of further guidelines under Article 26 of the CRA regarding the interaction between the CRA and Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA). As we have already noted in previous comments we call for clear exemption from the CRA for financial entities subject to DORA. We see an significant overlap between the Cyber Resilience Act (CRA) and the Digital Operational Resilience Act (DORA), which presents serious implementation challenges for the financial sector. DORA imposes stringent and comprehensive requirements on financial entities' ICT systems and services. DORA covers the entire lifecycle of these systems, from development to decommissioning, and includes risk-based management, incident handling, vulnerability management, and customer communication strategies.

Template document for comments to the draft Communication on Commission guidance on the application of the CRA

Organisation/individual	The German Banking Industry Committee (GBIC)
Date	01/04/2026
Other relevant info	The German Banking Industry Committee (GBIC) is the voice of the leading German banking-sector associations. These are the National

Instructions for the use of the template

If you are providing comments on a **figure**, please indicate the number of the figure (**F.x**); if you are providing comments on a **section** as a whole, or on a topic related to a specific section, please indicate the number of the section (**S.x**); if you are providing comments on a specific **paragraph**, please indicate the specific paragraph (**P.x**); if you are providing comments on a specific **example**, please indicate the number of the example (**E.x**).

If you wish to provide comments on a **topic that is not covered** by the draft guidance, please select "**Other topic**".

Organisation/individual	Item number	Comments	Proposed change
(Please enter the name of the organisation you represent or your name)	***(Please enter on which point you are commenting, as per above instructions. Allowed input: F.x; S.x; P.x; E.x; Other topic)***	***(Please enter your comment and a concise explanation or rationale.)***	***(Please enter your proposal (suggestion, modification, etc) as a text fragment for addition into the text or describe it as concise and precise as possible.)***

GBIC	F.9	As already communicated in a letter dated 8 July 2025 from the European banking associations to the European Commission, DG CNECT and DG FISMA: We see an significant overlap between the Cyber Resilience Act (CRA) and the Digital Operational Resilience Act (DORA), which presents serious implementation challenges for the financial sector. DORA imposes stringent and comprehensive requirements on financial entities' ICT systems and services. DORA covers the entire lifecycle of these systems, from development to decommissioning, and includes risk-based management, incident handling, vulnerability management, and customer communication strategies.	We support the issuance of further guidelines under Article 26 of the CRA regarding the interaction between the CRA and Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA). We call for clear exemption from the CRA for financial entities subject to DORA.
GBIC	S.5	Paragraphs 114–120 states that the support period must comply with Article 13(8), that the minimum support period is five years unless the expected use time is shorter, and that for software products manufacturers may, under certain conditions, address vulnerabilities only for the latest version if users can upgrade free of charge and without incurring "additional costs." The Annex also clarifies in paragraph 119 that reasonable operational effort does not count as an additional cost. However, the Annex does not sufficiently address situations where an institution depends on third-party components whose vendor-defined support lifecycles are materially shorter than the periods envisaged in the CRA. In such cases, a institution may remain operationally dependent on a component even though it has no ability to require the supplier to extend the support period.	The guidance should clarify that where integrators rely on third-party components with supplier-defined support lifecycles that they cannot control, compliance may be demonstrated through: - compensating controls, - segmentation, - accelerated replacement planning, and - risk-based decommissioning. The guidance should avoid implying that an integrator must guarantee a support period that it cannot enforce contractually or technically.

GBIC	S.7.3	In Section 7.3 is stated that manufacturers must carry out a cybersecurity risk assessment for the product and exercise due diligence with respect to integrated third-party components. It also states in paragraph 156 that third-party components are treated as external inputs whose properties must be verified upon integration because they cannot be re-designed or re-developed by the manufacturer. In Section 9.2.1 the Annex further provides that vulnerabilities in integrated components must be reported upstream, and that security fixes must be shared where the manufacturer has itself developed such a fix. Figure 9 illustrates this risk assessment / due diligence logic, and Figure 11 illustrates it in the context of a banking application using third-party services. However, the Annex does not clearly distinguish between: - the obligation to manage the risk of third-party components, and - an obligation to remediate the vulnerability inside the third-party component itself. For financial institutions, this distinction is crucial because many integrated components (cloud services, operating systems, vendor software, SDKs, firmware, cryptographic modules) cannot be legally or technically modified by the institution.	Institutions can manage the risk around third-party components, but they should not be expected to repair or rewrite components they do not own or control. That responsibility should remain with the original vendor. The guidance should clarify expressly that where an integrator cannot legally or technically modify a third-party component, its obligation is limited to: - due diligence, - applying supplier fixes, - monitoring advisories, - implementing compensating controls, and - managing residual risk at product level. The obligation to remediate the vulnerability inside the third-party component should remain with the component manufacturer or software vendor.

GBIC	S.9	Paragraph 193–197 state that reporting starts once the manufacturer has “become aware” of an actively exploited vulnerability or a severe incident, and that awareness exists when, after an initial assessment, the manufacturer has a “reasonable degree of certainty.” Section 9.2.2 explains when an exploitable vulnerability may be considered “known,” including where it is listed in public vulnerability databases or communicated through non-public channels. However, while the Annex explains when reporting timelines start and when a vulnerability may be considered known, it does not provide operational criteria for distinguishing between: - a suspicious event, - an actively exploited vulnerability, and - a severe incident having an impact on product security. In complex, integrated multi-vendor environments typical of the financial sector, this creates uncertainty as to how to classify events consistently and how to align CRA reporting with existing reporting regimes. Further in Section 9.1 is stated "manufacturers are required to inform impacted users and, where appropiate, all users" This doesn't provide the level of detail needed and the criteria who should be informed about what exactly.	We need clearer and more practical guidance on how to classify events, so that banks know exactly what to report and under which category. The guidance should include a practical decision framework that distinguishes: - suspicious events, - actively exploited vulnerabilities, and - severe incidents. It should define what level of evidence is sufficient for a “reasonable degree of certainty” and should align those concepts, as far as possible, with DORA and national incident reporting practices. Further, it should be clearly defined which users need to be informed. By informing "all users" we could propagate information of the vulnerability, increasing the risk (need to know principle).

GBIC	S.9.1	Paragraph 197 stated that manufacturers must submit an early warning within 24 hours, a 72-hour notification, and a final report within the prescribed deadlines. Paragraphs 193–200 explain the staged reporting logic and the obligation to inform impacted users where appropriate. However, the Annex does not provide standardised templates, minimum data fields, data schemas, or worked examples for any of these reporting stages. For financial institutions, this creates operational uncertainty because CRA reporting will need to be embedded into existing incident-management workflows, case-management tools, and reporting processes already used for DORA and national frameworks.	The Commission should provide practical templates and examples early on, so entities can prepare their reporting processes in a consistent way. The guidance should be supplemented with standardised reporting templates, minimum mandatory fields, and machine-readable schemas (for example for structured submission), together with worked examples for the 24-hour warning, 72-hour notification, and final report. These should be made available sufficiently ahead of go-live to support implementation and alignment with DORA and national incident reporting frameworks.

GBIC	Other topic	Article 21 CRA classifies distributors as manufacturers under certain conditions, including where they place a product with digital elements on the market under their own name or brand. Banking apps and payment cards are produced by a small number of manufacturers in Germany - but made available to bank customers by hundreds of banks. Distributors in the banking sector frequently brand a manufacturer's product with their own brand and make this product available to their customers for use without modification (e.g. banking apps, POS-terminals or payment cards). The actual manufacturer of the product remains identifiable and the manufacturer's product is not substantially altered. It is not appropriate in this case to transfer all manufacturer requirements to the banks as distributors. Among other things, each bank would have to draw up a declaration of conformity for one and the same product (for example, arrange for certification in the case of critical products). In the event of exploited vulnerabilities, instead of a single report from the manufacturer, each bank would have to report the same vulnerability in the same underlying product. This does not add value, but rather results in a proliferation of vulnerability reports from which it is not apparent that they refer to one and the same vulnerability.	It should be clarified that, in cases where a distributor merely labels a product from the actual manufacturer with its own name or brand, but the actual manufacturer remains identifiable on the product and no further changes are made to the product, the condition set out in Article 21 of the CRA is not met. In this case, the obligations under Articles 13 and 14 of the CRA should continue to rest with the actual manufacturer.