

EBF position on the Regulation revising the Cybersecurity Act (CSA2)

Introduction

On 20 January 2026, the European Commission published a Cybersecurity Act Review package, including two specific proposals: a Regulation revising the Cybersecurity Act (CSA2), and a Directive with targeted amendments to the NIS2 Directive (EU) 2022/2555.

The European Banking Federation strongly supports the goal of simplifying and harmonizing the EU legal framework and efforts by the European Commission to ensure proportionality, practical applicability and consistency across horizontal and sectorial frameworks.

1. Trusted EU ICT supply chain framework

The CSA2 proposal introduces a new Union-level trusted ICT supply chain security framework designed to reduce cybersecurity risks in ICT supply chains, particularly those linked to non-technical risks and dependencies involving third-country suppliers. For the banking sector, the European Commission's proposal for the CSA2 represents a shift from the risk-based approach established under the **Digital Operational Resilience Act (DORA)** to a non-technical risk framework. While DORA focuses on technical resilience and robust oversight by the European Supervisory Authorities (ESAs), CSA2 introduces rights for the European Commission to prohibit specific ICT suppliers based on geopolitical and non-technical risks.

Non-technical risks are described in the NIS Cooperation Group's Toolbox on ICT supply chain security. These include risks such as vendor lock-in and cybersecurity attacks on Cloud Service Providers. CSA2, however, goes further. The approach proposed under the CSA2 would create uncertainty within the private sector concerning what suppliers could be in-scope of such framework.

Additional clarity would be beneficial regarding the methodology and governance used to identify and designate high-risk suppliers and third countries posing cybersecurity concerns. Given the complexity of global ICT supply chains, predictability and transparency in such designation processes would be essential to allow entities to appropriately manage supply chain dependencies and plan mitigation actions.

The EBF notes a significant normative ambiguity regarding the geographical application of the proposed trusted ICT supply chain framework to the global operations of a Union-headquartered financial entities. Specifically, the framework lacks clear guidance on whether restrictive measures concerning designated providers extend to infrastructure located in **third-country jurisdictions**, particularly where such entities face a conflict of

laws or manifest market unavailability. Under the current draft proposal, the Union-based financial entities risk being placed at a competitive disadvantage.

Finally, we share a concern whether the designation of high-risk suppliers, together with the associated restrictions, could lead to a potential concentration at EU level on a small number of “trusted” suppliers, with a consequent increase in prices and the creation of new single points of failure. The EBF calls to the Legislator to consider phased approach, starting with the feasibility assessment and market capacity analyses to address such measures before imposing broad restrictions.

Identification of key ICT assets (Art. 102 CSA2): If certain critical components are prohibited across the EU, sufficiently long transition periods should at a minimum be provided to avoid adverse impacts on banks’ business activities and the continuity of their ICT operations. Furthermore, exemptions or hardship provisions should be established in cases where no viable alternatives are available to the institution. This designation process could also create complexity or duplication in cases where the Commission’s identification of key ICT assets does not align with the mapping carried out under DORA provisions. It should therefore be clarified whether requests for evidence on ICT dependencies and assets from banks would be issued, even though this information is already collected by the European Supervisory Authority for DORA compliance purposes.

Mitigation measures in the ICT supply chain (Art. 103 CSA2): The proposal also empowers the Commission to impose a wide range of mitigating measures affecting entities’ ICT supply chains, including restrictions on contractual relations with suppliers, technical configuration requirements, restrictions on remote access and requirements for supply diversification. For highly digitalised sectors such as financial services, these measures could have significant operational implications for outsourcing models, cloud adoption strategies and ICT architecture. The risk-based approach established by DORA and banks’ strategic decisions to invest on technologies and manage such risks should therefore be recognized. In this context, mitigation measures should be based on a feasibility assessment and market capacity analyses, and proportionate allowing flexibility to reduce the risk of unintended operational disruption.

The EBF calls the Legislator to consider that the mitigation measures should be taken in consultation with impacted/relevant stakeholders in order to anticipate any interdiction or other mitigating measures and to avoid them loss-making investments. It should be noted that the NIS Cooperation Group does not represent financial sector authorities.

Financial sector is already subject to a comprehensive framework for ICT third-party risk management under DORA, including the designation and oversight of critical ICT third-party service providers at Union level. Clear articulation of the relationship between these frameworks would help avoid overlapping supervisory expectations or conflicting obligations.

2. Strengthened role for the European Union Agency for Cybersecurity (ENISA)

The proposal aims to strengthen ENISA's role in supporting the effective implementation of EU cybersecurity policy and in enhancing operational cooperation between Member States. To this end, ENISA's mandate is reinforced with a range of new and expanded tasks. In parallel, the proposal revises ENISA's governance and resources to ensure they align with these expanded responsibilities.

We note that ENISA's mandate to support the sectors identified under NIS2 Directive must be sustained and further evolved. While the current sectors' maturity assessment framework established by ENISA¹ provides a robust baseline for identifying systemic needs, ENISA's focus should not be confined to capacity-building for less mature sectors.

It is critical that the Agency maintains its engagement with highly mature sectors, including the financial sector, in particular to drive two strategic objectives: (1) to provide technological foresight regarding the cybersecurity implications of emerging innovations; and (2) to ensure regulatory coherence at the nexus of horizontal policies and sectoral implementations.

Such dual approach in the mandate of ENISA would ensure that the EU cybersecurity posture remains proactive rather than reactive, and **would ensure that horizontal cybersecurity initiatives remain aligned with sector-specific regulatory frameworks and operational realities.**

3. European cybersecurity certification

The EBF already stated in its earlier positions in relation to the cybersecurity certification schemes that the drafting and adoption process of such European scheme **should be a purely technical process**, with a content that details technical requirements for a certification scheme.

Under CSA2, a request to issue a scheme and its adoption remains in the remit of the European Commission. **However, the transparency requirements** about steps and throughout all process when drafting a scheme remain rather generic.

We therefore call on the legislators to clarify how European cybersecurity certification schemes may interact with sector-specific regulatory requirements. For entities subject to multiple cybersecurity frameworks, including the financial sector, alignment between certification schemes and existing supervisory expectations is critical and it would help avoid duplicative compliance efforts.

From a simplification perspective, it would be desirable for such certification to also serve as evidence of the security measures required under DORA. Further clarification is also needed on how a single EU wide certification standard could effectively harmonize any detailed security requirements that Member States may introduce at the national level though transposition of NIS2, for instance.

Finally, we would welcome greater clarity regarding **the interplay between the European certification scheme and the proposed Union-level trusted ICT supply chain security framework**. The current wording of Article 100 (5) of the CSA2 does not address how withdrawal or de-risking measures adopted under the proposed Trusted ICT supply chain framework would relate to existing or future Union cybersecurity certificates. In the absence of further clarification, questions may arise as to the practical implications of such measures for certified products or services and for the continued applicability of certificates, which could benefit from additional guidance to ensure coherent application of the Regulation.

¹ <https://www.enisa.europa.eu/news/enisa-nis360-2024-report>

4. Incidents notifications scheme and proposal for Single-Entry Point under the Digital Omnibus

We note that the parallel legislative process for the Digital Omnibus for the incidents notification provisions shall strongly align with the CSA2 provisions. The two parallel streams add unnecessary complexity. In relation to the Single-Entry Point proposal, the EBF has issued a specific position (EBF_046988)

For more information:

Alexandra Maniati

Senior Director - Innovation & Cybersecurity

a.maniati@ebf.eu

Ingrida Taurina

Senior Policy Adviser - Innovation &

Cybersecurity

i.taurina@ebf.eu

About the EBF

The European Banking Federation is the voice of the European banking sector, bringing together 33 national banking associations in Europe that together represent a significant majority of all banking assets in Europe, with 3,500 banks - large and small, wholesale and retail, local and international – while employing approximately two million people. Launched in 1960, the EBF is committed to a single market for financial services in the European Union and to supporting policies that foster economic growth.