Proposal for a Cyber Resilience Act

Updated Position paper

Feedback on ITRE and IMCO amendments

July 2023

INTRODUCTION

TIC Council, the global trade association representing independent third-party testing, inspection, and certification (TIC) organisations, welcomes the work in the European Parliament but recommends further discussions to advance cyber resilience and cybersecurity for the future.

TIC companies provide independent conformity assessment services, verifying that products comply with the relevant essential requirements, and are therefore safe and secure before being placed on the market.

Under the Cyber Resilience Act (CRA), accredited TIC companies, referred to as Notified Bodies in the New Legislative Framework (NLF), have a crucial role in guaranteeing that the products undergoing independent conformity assessment procedures do indeed comply with the CRA's requirements. In other words, when Notified Bodies are involved in the conformity assessment process, they act as a prerequisite for market access, ensuring that only products meeting the CRA's cybersecurity requirements can enter the EU market.

TIC Council particularly welcomes the increased alignment of the CRA proposal with existing EU cybersecurity legislation, notably the EU Cybersecurity Act[1] (CSA) through the presumption of conformity for levels 'substantial' and 'high'. Adopting the CSA's mechanisms avoids duplication of work while supporting the industry's existing investments. This logic should be extended to other aspects of the CRA.

However, while negotiations on the text are ongoing, TIC Council suggests the following steps to ensure the CRA achieves its stated objectives:

1. **Further work to develop a robust and transparent product classification system.**

2. **Rejecting the postponement of the deadlines for implementing the text or the mandatory conformity assessment methods.**

3. **Fully recognising the TIC industry as a trusted partner with deep expertise in cybersecurity conformity assessment.**

[1] Regulation (EU) 2019/881 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification (Cybersecurity Act)

Further work to develop a robust and transparent product classification system.

The methodology for cybersecurity risk assessment and product classification in Article 6 should be rewritten in a transparent manner. This will give manufacturers and users legal certainty that the highest level of cybersecurity is being pursued, in line with the risk-based approach also outlined in Article 24.

To achieve this, Article 6 must define a product classification methodology based on transparent criteria and clear definitions that consider different levels of risk. The current amendments proposed by the ITRE Committee do not adequately address this issue. However, we support the amendment proposed by the IMCO Committee, which suggests grouping critical products into a single class. This aligns with our initial position[2] of including more products in the critical classes, especially consumer IoT products, to avoid obvious and dangerous misclassifications.

Secondly, Article 6 must be drafted taking into account Article 24 and the precautionary and risk principles of the NLF. This will ensure that all critical products are subject to conformity assessment by an independent notified body.

In addition, the cybersecurity risk assessment method should be the result of a discussion involving cybersecurity experts from different sectors, including those from conformity assessment bodies (CABs). Such collaboration would reduce the uncertainty as to whether these classes respond to the cybersecurity threats currently observable on the market.

Additionally, the final classification of products must consider existing requirements in related legislation, such as the Machinery Regulation and the Artificial Intelligence Act. Alignment with these regulations will ensure that safety, security, and the corresponding conformity assessment procedures are aligned upwards with the legislation prescribing the highest level of protection.

Rejecting the postponement of the deadlines for implementing the text.

The postponement of the text's application or conformity assessment methods would hinder the already uneven adoption of cybersecurity standards by manufacturers.

We strongly reject the proposed amendments calling for deadline extensions, such as the postponement of conformity assessment procedures by 6 months when harmonised standards, common specifications and certification systems are not available **(Article 24(2)a)**; by 12 months when new product categories are added to Annex III **(Article 6(4))**; and a 2-year period between each amendment to the categories in Annex III **(Article 6(2))**. These delays cannot be justified either on cybersecurity grounds or for implementation reasons.

Firstly, these amendments are in contradiction with the principles of the NLF, which require the involvement of a notified body in conformity assessment processes, particularly when harmonised standards are not available. Then, Notified Bodies will be prepared to provide their services when the text enters into force, as they will

[2] https://www.tic-council.org/news-and-events/news/press-release-cyber-resilience-act-tic-council-welcomes-commission-proposal-and-responds-public-consultation

possess the necessary skills and accredited assessment processes, preventing issues of certifying CRA products. Furthermore, considering that the CRA imposes baseline cybersecurity requirements for all products, the aspects of the products to be tested and the conformity assessment procedures will remain consistent across different product categories. Postponing the application of conformity assessment is unjustified, as it is the responsibility of manufacturers to promptly implement essential cybersecurity requirements that already apply to their other product categories within the CRA's scope.

Finally, it's important to have the flexibility to modify product classes to adapt to technological changes in an evidence-based manner without being bound by specific timelines.

Manufacturers can prepare for this transition now, enabling them to meet the initial application deadlines for the text and avoid promoting compromised products. Sticking to the initial application dates will ensure legal certainty and motivate manufacturers to prioritize the highest level of cybersecurity. Conversely, postponements will fuel cyber risks.

The independent TIC industry is a trusted partner with deep expertise in cybersecurity conformity assessment.

We reaffirm our commitment to being a trustworthy partner for manufacturers and partners in the cybersecurity sector. TIC companies have substantial experience in conducting cybersecurity assessments across various sectors and markets. Our members specialize in providing conformity assessment services as part of certification schemes such as ETSI EN 303 645 or the IEC 62443 series. In addition, manufacturers can be assured that TIC companies continually invest resources in training their staff with the latest state-of-the-art cybersecurity techniques.

In view of this, we request the co-legislators to remove the reference in **Article 29(7)(a)** that suggests the need to verify the skills of the conformity assessment body staff: if there is a lack or shortage of competent cybersecurity experts, it is an industry-wide problem. Additionally, CABs should be explicitly recognized as relevant stakeholders in the European Commission's expert group on Cyber Resilience, established under **Article 6a** of the CRA.

The independent TIC industry is a valuable business facilitator and trusted partner that support compliance obligations and cybersecurity. It is crucial for all stakeholders to keep in mind that the ultimate goal of the Cyber Resilience Act is to maximise the cybersecurity and resilience of the EU market.

Contact person: Mann Nguyen, Digital Policy Manager

Rue du Commerce 20/22, B-1000 Brussels
tel: +32 490 57 69 54
email: mnguyen@tic-council.org

TIC Council is the global trade federation representing the independent third-party Testing, Inspection and Certification (TIC) industry which brings together about a 100 member companies and organizations from around the world to speak with one voice. Its members provide services across a wide range of sectors: consumer products, security, medical devices, petroleum, mining and metals, food, and agriculture among others. Through the provision of these services, TIC Council members assure that not only regulatory requirements are met, but also that reliability, economic value, and sustainability are enhanced. TIC Council's members are present in more than 160 countries and the wider TIC sector currently employs more than 1 million people across the globe.