DIGITALEUROPE

02 December 2024

Recommendations on updated draft CRA standardisation request

Introduction

DIGITALEUROPE presents its perspective on the newly revised draft standardisation request supporting the Cyber Resilience Act (CRA).[1]

Building on our previous recommendations, which remain insufficiently addressed in the updated draft, this paper outlines additional proposals to reflect the latest changes.

Incorporating these recommendations is essential to facilitate the effective implementation of this groundbreaking mandatory framework for cybersecurity requirements in hardware and software:

- **'Security interests of the Union'**: The newly introduced Art. 2 lacks clear criteria defining the 'security interests of the Union,' creating ambiguity that raises concerns about proportionality and alignment with the Standardisation Regulation.[2] We call for clarification of these criteria or reconsideration of Art. 2 and Recital 13 to ensure coherence with stakeholder participation principles.

- **ETSI's role**: The European Telecommunications Standards Institute (ETSI) must be explicitly included in the standardisation request for all relevant entries. ETSI's expertise in telecoms and cybersecurity is essential for delivering robust, market-relevant and globally aligned standards.

- **Alignment with existing standards**: To streamline implementation, the CRA should leverage existing international standards rather than creating new frameworks. The request should be outcome-focused, avoiding rigid sequencing between vertical and horizontal standards to ensure consistency without unnecessary delays.

- **Realistic timelines**: The current draft imposes a sequencing requirement that delays the development of vertical standards until horizontal standards are finalised. This, coupled with misaligned

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202402847.

[2] Regulation (EU) 1025/2012.

deadlines, risks leaving manufacturers without adequate time to adopt standards before the CRA's application date. We recommend allocating sufficient time for standards development and aligning timelines with realistic industry needs.

- **Impact of open source on CRA standardisation**: There is a critical need for greater open-source software (OSS) expertise in the standardisation process. Whilst the draft acknowledges OSS participation, many OSS organisations lack the resources to engage effectively.

Table of contents

‘Security interests of the Union’

The newly introduced Art. 2 on the ‘security interests of the Union’ lacks clarity regarding the criteria defining these interests. This ambiguity makes it difficult to evaluate whether the proposed measures are appropriate and necessary, raising concerns about their alignment with the principle of proportionality.

Moreover, this article risks conflicting with the Standardisation Regulation, particularly Art. 5, which requires European standardisation organisations to ‘encourage and facilitate an appropriate representation and effective participation of all relevant stakeholders.’ The requirement for stakeholders to adhere to undefined security interests may inadvertently undermine this principle.

To avoid such contradictions, it is crucial to clarify the criteria defining the ‘security interests of the Union.’ In the absence of such clarification, we strongly recommend reconsidering Art. 2 and related Recital 13 to ensure coherence with the Standardisation Regulation and stakeholders’ effective participation in the standardisation process.

ETSI’s role

ETSI should be explicitly included in the draft standardisation request supporting the CRA. ETSI plays a pivotal role in developing cybersecurity standards within the EU, and its involvement is essential to establishing a balanced, effective and comprehensive standardisation framework. ETSI’s expertise in telecoms and cybersecurity ensures that the resulting standards are technically robust, market-relevant and aligned with global norms.

To fully leverage ETSI’s capabilities, the standardisation request must explicitly recognise and integrate ETSI’s role alongside other European standardisation organisations. Such inclusion would reflect the Standardisation Regulation’s principles of inclusivity and stakeholder participation, helping to deliver standards that are both robust and broadly applicable. Whilst ETSI is already referenced for entries 16–38 in Annex I, this acknowledgment should be extended to entries 1–15 and 39–41, ensuring ETSI is consulted as a liaison to provide its expert opinion across the full range of entries.

Furthermore, we reiterate several of our prior recommendations that remain insufficiently addressed in the newly updated draft standardisation request.

Alignment with existing standards

As we have consistently argued, reusing existing international standards – as opposed to building a completely new framework of standards – would greatly facilitate industry’s ability to comply with CRA requirements.

The CRA standardisation effort needs to draw from and augment existing standards to fulfil the standardisation request's goal of addressing the CRA's essential security requirements.

Whilst the standardisation request acknowledges international standards, the dependency requirement between vertical and horizontal standards may effectively hinder the practicality of this acknowledgment.[3]

The standardisation request should be outcome focused – it should not specify sequencing for the work but instead focus on the outcome, ensuring vertical standards are consistent with horizontal standards, with justified exceptions, regardless of which the standardisers start first.

Realistic timeline

The language in Annex II, paragraph 2.1 poses significant challenges. As currently drafted, it mandates that the development of any vertical standard can only begin once horizontal standards are available, due to the use of the term 'shall.' This sequencing requirement would substantially prolong the standardisation process, making it difficult for standardisers to deliver robust standards within the already tight CRA timelines. Such delays would cause significant negative impacts on the market.

The draft standardisation request specifies deadlines for standards availability, but these are misaligned with the CRA's proposed timelines. Considering that the CRA applies from December 2027, 13 out of 15 horizontal standards will only be ready by 30 October 2027 – just days before the CRA's application date. This timeline leaves manufacturers with no transitional period to adopt and implement the standards, forcing many to rely on alternative technical specifications for compliance. This undermines the level playing field within the single market, particularly for SMEs, and complicates compliance assessments for market surveillance authorities.

DIGITALEUROPE urges the Commission to learn from past experience, notably the delays in developing standards for the RED delegated regulation.[4] In that case, an initial two-year timeline for three standards had to be extended by an additional year despite considerable effort and resources. Similar risks arise with the CRA. Should an unrealistic timeline for developing standards persist, the CRA's implementation will face similar delays or challenges, disrupting its intended objectives.

To avoid such issues, harmonised and cited standards must be ready well before the CRA's applicability date. Standards development is inherently time-consuming, requiring open, transparent and consensus-driven processes,

[3] This also contradicts statements on the use of international standards for the CRA made by the European Commission during previous meetings of CEN-CENELEC JTC 13 WG9.

[4] Commission Delegated Regulation (EU) 2022/30.

alongside adequate consultation periods. The current timelines do not sufficiently account for these needs.

DIGITALEUROPE recommends the inclusion of provisions in the standardisation request to support ESOs in expediting the development of necessary standards. This could include:

- Allocating additional resources and support mechanisms to ESOs;
- Providing timely and clear interpretative guidance on the CRA’s legal text; and
- Offering responsive answers to standardisation-related questions to minimise delays and ensure standards meet both market and Commission expectations.

Further complicating matters, conformity assessment bodies have limited capacity to handle the CRA’s broad scope of mandated assessments. This issue will be exacerbated by the lack of harmonised standards granting presumption of conformity, particularly for Class I products in Annex III. Bottlenecks in third-party conformity assessments will heavily impact manufacturers requiring certification, straining the system further.

Additionally, the CRA envisions secondary legislation to define critical and important product categories within 12 months of its entry into force. This tight timeline creates uncertainty for standardisers, who will lack the necessary legal references to begin developing specific vertical standards. Without clear guidance on product categories, time pressures on the entire standardisation process will only intensify.

Impact of open source on CRA standardisation

A widely recognised and critical knowledge gap amongst stakeholders is the need for greater expertise in OSS and more open approaches to standardisation.[5]

Whilst the current draft standardisation request requires effective participation from OSS communities, significant uncertainty remains regarding their capacity to engage meaningfully in the CEN-CENELEC and ETSI standardisation processes. Many OSS organisations face operational and financial constraints that limit their ability to contribute effectively to these efforts.

Some of our members are taking proactive steps to reengage in the standardisation process, bringing much-needed OSS expertise to the table. However, these efforts continue to be met with considerable challenges.

[5] Largely developed through fora and consortia such as Oasis, IEEE and IETF as well as open foundations such as Eclipse, Linux Foundation, Apache and OWASP.

FOR MORE INFORMATION, PLEASE CONTACT:

Rita Jonušaitė

Senior Manager for Cybersecurity & Cloud

rita.jonusaite@digitaleurope.org / +32 499 70 86 25

Sid Hollman

Policy Officer for Cybersecurity & Digital Infrastructure

sid.hollman@digitaleurope.org / +32 491 37 28 73

About DIGITALEUROPE

DIGITALEUROPE is the leading trade association representing digitally transforming industries in Europe. We stand for a regulatory environment that enables European businesses and citizens to prosper from digital technologies. We wish Europe to grow, attract, and sustain the world's best digital talents and technology companies. Together with our members, we shape the industry policy positions on all relevant legislative matters and contribute to the development and implementation of relevant EU policies. Our membership represents over 45,000 businesses that operate and invest in Europe. It includes 113 corporations that are global leaders in their field of activity, as well as 41 national trade associations from across Europe.