DIGITALEUROPE

15 MAY 2024

Recommendations on revised draft CRA standardisation request

Introduction

DIGITALEUROPE welcomes the opportunity to share its views on the revised draft standardisation request in support of the Cyber Resilience Act (CRA).[1]

In this paper, we put forward our high-level recommendations to ensure a timely availability of robust standards in support of the CRA. Addressing these recommendations is crucial to ensure a smooth implementation of this world-first mandatory framework of cybersecurity requirements for hardware and software.

Table of contents

[1] https://ec.europa.eu/docsroom/documents/58974.

DIGITALEUROPE
Rue de la Science, 37, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

Alignment with existing standards

As we have consistently argued,[2] rather than building a completely new framework of standards, reusing existing international standards would ensure timely and smoother implementation of the CRA, facilitating 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 essential security requirements. The revised draft standardisation request puts forward significant changes that potentially undermine this fundamental goal.

One significant change is the requirement that '[v]ertical standards developed under this request *shall* therefore build on and further specify the horizontal provisions.'[3] This would complicate the possibility of developing harmonised standards based on existing, proven European and international standards. It would also risk a decoupling from international standards, which would negatively impact Europe's global competitiveness.[4]

Whilst the standardisation request acknowledges international standards, the dependency requirement between vertical and horizontal standards may effectively hinder the practicality of this acknowledgment.[5] 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 change of language in Annex II, paragraph 2.1 would mean that the development of any vertical standard can only start after the availability of the

---

[2] See *Setting the standard: How to secure the Internet of Things*, available at https://cdn.digitaleurope.org/uploads/2021/09/DIGITALEUROPE_Setting-the-standard_How-to-secure-the-Internet-of-Things.pdf.

[3] Annex II, paragraph 2.1, our emphasis.

[4] For example, EN IEC 62443, identified as useful to CRA standardisation by the Joint Research Centre (JRC) and ENISA and included in the Rolling Plan for ICT Standardisation, is an example of an established standard whose possible function as a basis for CRA standards would be compromised under the current draft standardisation request. See *Cyber Resilience Act Requirements Standards Mapping: Joint Research Centre & ENISA Joint Analysis*, available at https://www.enisa.europa.eu/publications/cyber-resilience-act-requirements-standards-mapping and https://joinup.ec.europa.eu/collection/rolling-plan-ict-standardisation/rolling-plan-2024, respectively. The standardisation request should allow for a complete standards series rather than some parts, as the joint JRC-ENISA mapping exercise has done for EN IEC 62443. Standards series provide a comprehensive framework for implementors, which allow better application, especially as no reasons were given as to why some parts were excluded.

[5] 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.

horizontal standards. This would require significantly more time for standardisers to establish robust standards in support of the CRA. As the envisioned CRA timeframes are already tight, this would lead to real negative market impact.

Conformity assessment bodies face limited capacity to perform all conformity assessments mandated by the CRA's large scope. This would be compounded by the absence of harmonised standards providing presumption of conformity for categories listed in Class I of Annex III, which would generate further bottlenecks for third-party conformity assessments of these products, too. Manufacturers whose products require third-party certification would also be heavily impacted.

Moreover, the CRA foresees secondary legislation to provide legal clarity as to a very broad and largely undefined set of important or critical products within 12 months of entry into force. This approach will not allow standards to progress properly as they will lack reference to this first layer of secondary legislation having first been completed. Until such time, standardisers will have no conclusive information on which specific vertical standards need to be developed for the CRA's product categories. This increases time pressure on the entire standardisation process.

At the same time, it is possible for a product to have several core functions in accordance with Annexes III-IV CRA. Although Art. 7(1) CRA refers to products' core functions as the central classification criteria, some manufacturers are still unclear as to which categories their products fall into. This exposes manufacturers to double regulation and contradictory requirements from vertical standards. Equally, though not legally required, economic operators – and specifically notified bodies – are dependent on harmonised standards.

The draft standardisation request specifies deadlines by which the standards are to be available. However, provided the CRA is published in the Official Journal of the EU (OJEU) by October 2024 at the latest, and thus applies from October 2027, 13 out of 15 horizontal standards will only be ready after the CRA's application date, as their deadline is 30 October 2027. Manufacturers need time to prepare for, adopt and implement standards.

DIGITALEUROPE insists that lessons be learned from the work delivered in JTC13 WG8 on standards in support of the RED delegated regulation, where an initial timeline of two years to develop three standards had to be extended by one year, despite enormous additional investments of time and efforts by standardisers.[6]

This work should also form the basis for horizontal standards in support of the CRA to maximise efficiency and ensure they are developed and delivered in a shorter timeframe, allowing for vertical standards to be developed well before

[6] Commission Delegated Regulation (EU) 2023/2444 amending Delegated Regulation (EU) 2022/30.

the 30 October 2026 deadline. Vertical harmonised and cited standards must be ready and available in good time before the CRA becomes applicable. Therefore, we need to ensure that they can be developed in a timely manner.

Impact of open source on CRA standardisation

A related and significant knowledge gap widely identified by all relevant stakeholders is the need for more open-source-software (OSS) expertise and open standardisation.[7]

Even if effective participation of OSS communities is required in the current draft standardisation request, there exists significant uncertainty as to whether such organisations have the operational bandwidth and financial capacity to get involved in the CEN-CENELEC standardisation development process. Some of our members are taking additional steps to re-engage in this process to provide much needed OSS expertise, but the challenges are considerable.

Different nature of conformity assessment modules

Conformity with the CRA's essential requirements is to be reached through the conformity assessment procedures under Modules A, B, C and/or H set out in Annex VIII.

Annex I, paragraph I of the draft standardisation request stipulates that 'the standard must cover the conformity assessment modules as defined in the CRA.' We should be cognisant of the fact that the aforementioned modules, however, are different in nature.

Module H focuses on the manufacturer's quality management system, which ensures compliance with the essential requirements of the CRA. Modules A, B and C, on the other hand, address the fulfilment of the actual essential requirements.

From a standardisation perspective, it is not achievable to address both quality management system requirements and functional/process requirements derived from Annex I CRA in a single standard. Consequently, DIGITALEUROPE strongly recommends deletion of references to specific modules.

[7] 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 108 corporations that are global leaders in their field of activity, as well as 41 national trade associations from across Europe.