DIGITALEUROPE

22 SEPTEMBER 2023

Building a strong foundation for the Cyber Resilience Act: key considerations for trilogues

Executive summary

Trilogues on the proposed Cyber Resilience Act (CRA) will set the foundations for a world-first framework of mandatory cybersecurity requirements for 'products with digital elements.'[1]

For the CRA to meet its objectives, the final text must include measures that make compliance clear and actionable, rather than generate new uncertainties that would disrupt Europe's ability to innovate and compete globally.

Current estimates put the global cybersecurity workforce gap at 3.4 million people, with Europe lacking more than 200,000 cyber professionals.[2] It is crucial to avoid unrealistic pre-market approval and compliance demands for such a huge scope of hardware and software products used and developed by private and public entities. These demands – as a whole and individually – will, in many cases, only work to undermine the legitimate investment required to increase cybersecurity.

For an effective CRA, the following aspects must be considered during trilogues:

- An **implementation period of at least 48 months** should be provided so that the necessary harmonised standards can be developed, and to avoid a bottleneck of third-party assessments due to a lack of capacity and/or technical competence;
- The **specificities of software** should be factored in when using traditional concepts from the New Legislative Framework (NLF). The final text can further specify some concepts, such as 'substantial

[1] COM(2022) 454 final. For our full position on the Commission's proposal, see DIGITALEUROPE, *Cybersecurity everywhere: deciphering the Cyber Resilience Act*, available at https://www.digitaleurope.org/resources/cybersecurity-everywhere-deciphering-the-cyber-resilience-act/.

[2] See the 2021 and 2022 ISC2 Cybersecurity Workforce Studies, available at https://www.isc2.org/research.

DIGITALEUROPE
Rue de la Science, 14A, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

modification,' and guidelines should be developed with input from a **newly created Stakeholder Expert Group**, which should advise the Commission on the CRA's implementation and future review;

- Criticality levels should ensure that **most products can undergo self-assessment**, leveraging harmonised standards and prioritising mutual recognition agreements (MRAs) to facilitate market access in third countries and allow for scalability;
- The **exclusion of open-source software** (OSS) must be refined so as not to discourage crucial upstream contributions by commercial entities. Similarly, **spare parts** that are intended to replace identical parts, as well as **websites** and **cloud services** covered by the NIS2 Directive should be excluded;[3]
- The **concept of 'partly completed product'** should be introduced to better address the nature of components, allowing for more accurate and efficient conformity assessment of software or hardware that must be incorporated into finished products;
- **Reporting obligations**, timelines and definitions must be aligned with the NIS2 Directive, focusing on significant incidents. The CRA should **not mandate reporting of unpatched vulnerabilities**. Instead, ENISA should establish a European catalogue of known exploited vulnerabilities, in coordination with already existing recognised initiatives;
- Provisions on **product security support** should allow manufacturers to determine the period of support, with the obligation to be transparent and taking into account product life expectancy and consumer expectations;
- The CRA must directly **repeal the Radio Equipment Directive (RED) delegated act on cybersecurity**,[4] which the CRA makes redundant, and provide for a transition period where compliance with either will be possible; and
- The **voluntary nature of cybersecurity certification schemes** should be retained. Approved schemes should be automatically recognised as a means for manufacturers to prove compliance.

[3] Directive (EU) 2022/2555.

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

Table of contents

Scope

A fundamental element to meet the CRA's objectives is a clear and enforceable scope, which should acknowledge the challenges of expanding the NLF to software and digital products whilst building on established risk management practices. Whilst both the European Parliament and the Council have taken steps in the right direction, a few crucial points must be addressed.

Open-source software

It is necessary to differentiate between the upstream and downstream use of OSS. Upstream use is the collaborative, collective contributions and releases of OSS, whereas downstream use requires configuring and compiling upstream code into a product which is commercialised onto the market.

The ITRE Committee's report does not yet reflect these important distinctions between downstream users and upstream contributors, with a middle layer of organisations that host or package OSS projects, as distinguished from products.

Art. 2(3a) stipulates that only OSS which is 'made available … in the course of a commercial activity' is within scope. However, OSS is predominantly 'commercial,' with millions of contributors ultimately working for companies (and governments) in the course of a commercial activity.

Furthermore, the recitals proposed by the ITRE Committee complicate the moment when this commercialisation is realised, and thus which entity should be held responsible for ensuring sufficient risk management to which upstream projects, libraries or tools they are integrating into their products.[5]

This creates a legal disincentive to European companies wanting to support and/or contribute more code upstream and/or the community itself receiving code contributions, which could include security enhancements. There is also a risk that ITRE's framing of OSS would qualify non-profit foundations as manufacturers.

The Council's general approach better reflects the OSS ecosystem by focusing on OSS that is supplied or integrated into a product placed on the market, as opposed to the open development phase envisaged by ITRE. As such, DIGITALEUROPE supports the Council's acknowledgement that employee-

[5] For instance, Recital 10b departs from the EU's 'default to open approach' by incorrectly qualifying upstream contribution as commercial if the developer is an employee and/or companies make financial contributions to upstream projects. The ITRE Committee effectively designates donations as a commercial activity when they are made by commercial entities and are recurring in nature, regardless of the legal posture of the entity receiving the funds and hosting or supporting the upstream activity.

developers working on upstream projects are key to open innovation and largely unrelated to the products that are subsequently placed on the market.[6]

We welcome both institutions' consensus to avoid inappropriately applying CRA responsibilities by the clarification 'most package managers, code hosting and collaboration platforms should not be considered as distributors.'

In addition, the final text should continue to allow for contractual agreements between OSS providers and manufacturers. For instance, the manufacturer may assume responsibility of the OSS or pass it through to the OSS provider.

In sum, to avoid overburdening the OSS community, and thus significantly disrupting a public good, **we urge EU trilogue negotiators that OSS should be exempted because it does not offer a 'product' on the market, and if it does not monetise its code**. Instead, the Commission should determine a potential extension of the scope in the future evaluation and review of the Regulation, after having assessed its impact and consulted the future Stakeholder Expert Group to decide whether OSS should be more stringently covered.

Spare parts

Ensuring that spare parts can still be delivered for legacy devices is pivotal to avoid shortages in existing critical infrastructure and industrial production lines. We **welcome the co-legislators' exclusion of spare parts** in their respective positions.

However, **it should be made explicitly clear** in Art. 2 that most spare parts are not exclusively manufactured, as they can be part of the same production and stored separately. Also, spare parts are not only provided by the product manufacturer, as environmental legislation encourages third-party spare parts.

Remote data processing

We welcome the co-legislators' efforts in Recitals 9 and 9a, which help clarify that websites that do not support the functionality of a product, or cloud services designed and developed outside the responsibility of a manufacturer, are not in the CRA's scope. This clarification should be reflected in the articles. We also support the exclusion of websites as well as the Council's clarification that "*requirements concerning the remote data processing solutions under the scope of this Regulation do not entail technical, operational and organisational*

[6] This said, the Council's exemption of entities recouping costs related to a service (as opposed to the software) would create a market distortion by rewarding a service provider who doesn't necessarily contribute upstream, or who bundles the 'free' upstream code into a broader platform service. Similarly, the proposed exemption for software 'developed or modified by a public authority' undermines the Council's supply-side focus and poses IP challenges, requiring changes to 'field of use' terms under many OSS licences.

measures aimed at managing the risks posed to the security of their network and information systems as a whole."

However, the inclusion of 'remote data processing' in the proposal's scope remains at odds with Recital 9's intention to exclude software as a service (SaaS), the latter already being regulated under NIS2.[7]

In order to circumscribe this inherent overlap, absent a full deletion of remote data processing from the scope, the definition in Art. 3(2) should **exclude the hardware, software and services used for remote data processing, transmission and storage**. This will ensure that at least IaaS and PaaS are not inadvertently included, and reflect Recital 9's intent in an operative provision to the effect that services in and of themselves are out of scope.[8]

Whilst this approach can help to reduce overlap with NIS2, it cannot fully resolve all challenges related to the intersection between SaaS and the notion of remote data processing. We urge that this issue should be further detailed in guidelines on software, with input from the suggested Stakeholder Expert Group, as proposed by the ITRE Committee.

Components

We welcome the IMCO Opinion's introduction of the concept of **'partly completed products with digital elements,'** as we advocated. This would build on the approach already taken in the Machinery Regulation.[9]

We call on co-legislators to consider the uncertainty that will result from a blanket inclusion of hardware and software components in the Regulation's scope, by treating them as if they were finished products. **Introducing the concept of 'partly completed products' would allow a more transparent and manageable supply-chain approach** that would benefit both component manufacturers and manufacturers of finished products.

This approach would introduce a dedicated, simplified conformity assessment procedure, resulting in a 'declaration of incorporation,' requiring manufacturers of partly completed products to identify essential requirements which, given the

[7] The CRA's explanatory memorandum states (pp. 2-3) that NIS2 ensures 'that technical specifications and measures similar to the essential cybersecurity requirements of the Cyber Resilience Act are also implemented for the design, development and vulnerability handling of software provided as a service (Software-as-a-Service).'

[8] This will also ensure that changes in infrastructure services do not require a new conformity assessment for products with digital elements when the infrastructure boundaries are commercially accessible, either through standardised interfaces or clearly documented integration points. We also note the inclusion of 'hypervisors and container runtime systems that support virtualised execution of operating systems and similar environments' in Class II of Annex III. However, IaaS provides virtual machine environments that are separated from each other precisely by hypervisors or container runtime systems. This might unintentionally bring IaaS into scope.

[9] See the definition of 'partly completed machinery' at Art. 3(10), Regulation (EU) 2023/1230.

partial nature of their products, cannot yet be addressed in their own conformity assessment but need to be assessed at a later stage.[10]

Adapting NLF concepts to software

The need to adapt existing NLF concepts, which were originally conceived for physical goods, to software and the dynamic nature of cybersecurity should not be underestimated, lest compliance efforts be made ineffectual.

The proposal sets out several obligations which are straightforward for tangible products, but which do not consider the specificities of software products.

As an example, the provision of security updates throughout the 'product lifetime' does not fit the logic nor the business practice of software products, which are often based on a monthly subscription or an annualised licence sales model. This has also been reflected in the Commission's evaluation of the NLF, which was published shortly after the CRA proposal.[11]

DIGITALEUROPE welcomes the **Parliament's proposal for the creation of a Stakeholder Expert Group (Art. 6a) and the development of guidelines (Art. 17a)** to clarify the application of NLF concepts in a software and cybersecurity context.

Amending and specifying criticality categories

Co-legislators have surprisingly maintained the Commission's leeway to further expand an already very broad scope with delegated and implementing acts.[12] Whilst a mechanism to update the list of critical products may be necessary, we insist that the CRA's initial scope should be clearly stated in the final text itself, and that **Art. 6(3) should therefore be deleted**.

As mentioned above, we welcome the Parliament's Art. 6a, which allows for the **Stakeholder Expert Group to advise the Commission on the exercise of its powers** – including, crucially, Art. 6(2) delegated acts.[13] **The need for a non-binding Opinion from this group should be reflected in Arts 50-51.**

---

[10] This approach is especially valuable for hardware products, whilst it might be less applicable to software, notably standalone software. Because of the broad definition of 'product with digital elements,' software is more likely to be in scope as a product as such, with flexibility in the application of the Annex I essential requirements being particularly important ('where applicable,' as we highlight in the 'Obligations and essential requirements' section below). This could also be addressed in the proposed guidelines on software.

[11] SWD(2022) 364 final.

[12] Arts 6(2) and (3).

[13] We note, in passing, that Art. 6(2)(c) mentions the 'processing of personal data' as a 'critical or sensitive function' that may justify incorporation in the list of critical products. The processing of personal data is so widespread that its mention, even as a non-exhaustive example, is moot. We suggest it should be deleted.

Conformity assessment

Workable conformity assessment processes will be pivotal to the CRA's practical implementation and success. Mandating third-party assessments for too many products, which will unnecessarily subject software to more testing than already takes place for many enterprise users, will result not only in delays bringing products to the European market and more expensive products, but also in a capacity shortage in notified bodies that may make market entry impossible altogether. Self-assessment should therefore be prioritised as much as possible over mandatory third-party assessment.

We welcome the **Council's reduction of the list of products in Annex III**, as well as both legislators' **recategorisation of some of products from Class II to Class I**, notably in the case of microprocessors.

Additionally, the Parliament's clarification in Art. 6(1) that **the integration of a product of higher class of criticality does not change the level of criticality for the product it is integrated into** is important and should be kept in the final text.

Harmonised standards

The existence of harmonised standards is necessary for reliable conformity assessment, including self-assessment, which should be maximised as argued above. The CRA must provide for the right conditions for such standards to be developed.

Given the CRA's wide scope and short implementation timelines, it is likely that many product groups **won't have harmonised standards available** by the time products will have to comply. This is relevant for products for which self-assessment against harmonised standards will be possible, but also for critical products which must undergo third-party assessment. Notified bodies, although not legally required, are dependent on harmonised standards, too.

Co-legislators must allow the time necessary for European standardisation organisations (ESOs) to deliver high-quality harmonised standards. **A realistic timeline for the development and adoption of harmonised standards is crucial.** We must learn from past mistakes – including, importantly, the RED delegated act on cybersecurity, whose applicability the Commission ultimately had to delay to reflect the actual timelines and processes involved in standardisation.[14]

The proposed 36 months makes it impossible for ESOs to have harmonised standards ready in time. Considering that **an absolute minimum of 24**

[14] The Commission last 20 July communicated to the expert group on Radio Equipment that it has delayed the date of applicability of Delegated Regulation (EU) 2022/30 until 1 August 2025.

months is needed only for their development, 48 months is the minimum needed for a solid transition period.

Cybersecurity certification schemes

The CRA should establish a straightforward and pragmatic route for manufacturers to rely on certification schemes adopted pursuant to the Cybersecurity Act,[15] should they wish to pursue certification rather than follow one of the NLF modules. Manufacturers should be free to choose whether to follow one of the NLF modules or to **voluntarily pursue cybersecurity certification as a means to prove compliance**.[16]

It is perplexing that EU schemes already approved by the Commission should only be presumed to ensure compliance with essential cybersecurity requirements only when their adequacy is reassessed and sanctioned in a separate act. Products certified pursuant to the Cybersecurity Act should automatically be presumed to be in conformity with the CRA's essential requirements.

As such, Art. 18(4) in the ITRE Committee report and Art. 18(10) requiring a separate delegated act to recognise EU cybersecurity certification schemes should be deleted, as should related references.

The Council has proposed a new category, Annex IIIa, for which the Commission can adopt delegated acts to determine which products will be required to obtain a European cybersecurity certificate at a specified assurance level (Art. 6a). In the absence of such delegated acts, the products that the Council lists under Annex IIIa will be required to go through third-party assessment. Equally, the Parliament's position is that the Commission can introduce, by means of a delegated act, a new list of highly critical products that will require a cybersecurity scheme at assurance level 'high' (Art. 6(5)).

As we have argued above, whilst CSA schemes should be used to prove compliance on a voluntary basis, introducing schemes in a mandatory fashion under NLF legislation will generate more uncertainty in the system. Using the NLF approach, if a product is in the future considered 'highly critical,' it should simply be included anew under Class II of Annex III to ensure a heightened level of scrutiny using third-party conformity assessment. This would not

[15] Regulation (EU) 2019/881.

[16] We note that the proposal to require an implementing act may have been driven by potential conflicts with mandatory third-party certification required for critical products under Class II of Annex III, as well as by concerns that certification schemes may not meet the CRA's essential requirements. However, we note that no schemes have been adopted to date, and that the only scheme about to be finalised (the EUCC scheme) does not include a self-assessment option. More broadly, alignment with the CRA's essential requirements, assurance levels and assessments will necessarily need to be factored in to any ongoing draft schemes now that the CRA has been proposed. We also note that the CRA should provide baseline requirements, cybersecurity schemes being able to go beyond them to achieve higher assurance.

exclude the possibility to use or develop cybersecurity schemes applicable to such products, which manufacturers could voluntarily comply with for the purposes of the CRA.

Therefore, **Art. 6(5) in the Parliament's text and Annex IIIa and Art. 6a in the Council's position should be deleted.**

Mutual recognition

The Parliament's proposed Art. 24a, introducing a mandate for the Commission to conclude and update mutual recognition agreements (MRAs) with third countries is an important and helpful addition that will facilitate market access.

We encourage the Council to support this proposal and to mandate the Commission to enter into negotiations with third countries as quickly as possible. The countries having an MRA covering the current RED could be a good start.

Obligations and essential requirements

Annex I and Art. 10 delineate obligations for economic operators and essential requirements that are largely in line with industry best practice. Furthermore, we welcome the recognition that essential requirements should apply 'where applicable,' which will allow product specificities to be taken into account based on a risk assessment.

Some of the obligations and requirements, however, should be clarified during trilogues.

Product security support

We welcome the ITRE Committee's balanced approach, which allows manufacturers to determine product support that is proportionate to the expected product lifetime, taking into account the nature of the product and users' expectations, amongst others. On the other hand, the Council's position is that vulnerability handling, including security support, should be mandatory during the expected product lifetime.

Given that some products are in use for decades, the 'expected lifetime' approach is not a sustainable option for manufacturers and goes against the original proposal's intention to improve baseline security. The **obligation to be transparent about the support period**, where applicable, is already a very important step and followed in other jurisdictions as well.[17] We therefore call on the Council to support the Parliament's balanced approach during negotiations.

[17] See the UK Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations 2023.

Substantial modification

Product support is closely linked to the concept of 'substantial modification,' which must ensure that **software updates are not unduly understood as requiring a new conformity assessment** or as extending the reference point for compliance. We welcome the Council's clarification under Recital 22a, aligned with the NLF's Blue Guide,[18] stipulating that security updates do not modify the intended purpose of a product and should not be considered a substantial modification.

The ITRE Committee has rightly also explicitly stated in Art. 3(31) that **necessary security updates that aim to mitigate vulnerabilities are not considered a substantial modification**. We call on co-legislators to include this clarification in the final text.

Aligning reporting to NIS2

Incidents

We welcome the Parliament's **focus on *significant* incidents only** in Art. 11(2), which is aligned with the language in Art. 23(1) NIS2 Directive, and call on the Council to support it. We further recommend that Recital 19 in both mandates be clarified, as it introduces disparities between the definition of 'incidents' (and 'vulnerabilities') used in NIS2 and those to be applied in the context of the CRA. In doing so, the CRA introduces legal uncertainty as the terms are defined in the articles by way of a direct cross-reference to NIS2, and so should be understood in the same way in both legislative acts.

Additionally, unlike proposed Art. 11(4), which obliges manufacturers to notify users about all incidents, the final CRA text should align to NIS2 by requiring, 'where appropriate,' notification to users of 'significant incidents that are likely to adversely affect' a product's security.[19]

We also welcome the Parliament's proposal in Art. 11(2c) for manufacturers that have notified significant incidents under the CRA, and who are essential or important entities under NIS2, to **be deemed compliant with the requirements under Art. 23 NIS2**. This measure is important to ensure alignment between the CRA and NIS2, and to avoid duplicative requirements for entities subject to both legislative acts. We therefore call on the Council to support this approach.

Vulnerabilities

[18] https://single-market-economy.ec.europa.eu/news/blue-guide-implementation-product-rules-2022-published-2022-06-29_en.

[19] Art. 23(1) NIS2 Directive. This would capture, for example, incidents that impact the integrity or confidentiality of the source code of software during the design and development phase, which are a source of supply chain attacks such as SolarWinds.

Mandatory reporting of 'actively exploited vulnerabilities,' as anticipated in the proposal, should be excluded.

Industry and consumer organisations alike have warned against premature reporting of unpatched vulnerabilities across the board,[20] which exposes products to new cybersecurity risks, in addition to deviating from established standards for coordinated vulnerability disclosure.[21] **We urge co-legislators to reconsider their approach and focus only on reporting of patched vulnerabilities that have been actively exploited and pose a significant cybersecurity risk.**

As with 'cyber threats' under NIS2,[22] manufacturers should **'where appropriate' communicate to potentially affected users any measures or remedies they can take** in response to a significant vulnerability. This is particularly important to allow for mitigation measures in a business-to-business (B2B) context.

If co-legislators insist on maintaining actively exploited vulnerabilities in scope, we ask for inclusion of a provision stating that, in exceptional circumstances, the **notification may be delayed based on justified cybersecurity-related grounds** for a period that is strictly necessary for the manufacturer to focus on mitigation. In practice, this could be reflected by amending the Council's proposed Art. 11(2c).

Additionally, the Council's proposed change to the definition of 'actively exploited vulnerability' to include **attempts** by a malicious to exploit the vulnerability, irrespective of whether the attempt was successful or not should be rejected. The change to 'attempts' is disproportionate and would contrast with international best practices. **We support the Commission and Parliament's definition**, whereby there must be reliable evidence that execution of malicious code was performed without the permission of the system owner.

We support the Parliament's **expansion of Recital 19**, clarifying that vulnerabilities discovered with no malicious intent for good-faith testing, investigation or correction should not be subject to mandatory notifications.

In addition, complementing the European vulnerability database created by Art. 12(2) NIS2, **ENISA should be tasked with establishing and maintaining a**

[20] See *Oversharing is not caring, it is a cyber risk: joint statement raising concerns on unpatched vulnerability reporting in the Cyber Resilience Act*, available at https://www.digitaleurope.org/news/oversharing-is-not-caring-it-is-a-cyber-risk-joint-statement-raising-concerns-on-unpatched-vulnerability-reporting-in-the-cyber-resilience-act/, and *Open Letter: Make vulnerability disclosure in the Cyber Resilience Act more secure, not less*, available at https://edri.org/our-work/open-letter-make-vulnerability-disclosure-in-the-cyber-resilience-act-more-secure-not-less/, respectively.

[21] ISO/IEC 29147, for example, requires disclosure only after the development and deployment of remediation.

[22] Art. 23(2), ibid.

European catalogue, aligned with its CISA equivalent,[23] **of known exploited vulnerabilities** which can be patched. Manufacturers should be required to report instances where their products contain vulnerabilities included in such catalogue.

This catalogue would build a picture of the landscape of high-risk vulnerabilities to be mitigated from a product perspective, and act as a central source of information about which of the many thousands of existing vulnerabilities are highest risk in practice and should be prioritised.[24]

When it comes to essential requirements, we welcome the Council's clarification in **Annex I.2(4)** allowing for **manufacturers, in duly justified cases and where they consider the security risks of publication to outweigh the security benefits, to delay making information regarding a fixed vulnerability public until after users have been given the possibility to apply the relevant patch.** The same flexibility should be followed in Art. 11.

In Annex I(1)(2), we welcome the risk-based approach as well as the deletion of 'delivered' by both Parliament and Council. We find that further clarity should be added in a new recital stipulating that **initial patching at the time of putting into service is sufficient** to fulfil this requirement, which is also reinforced by the helpful amendment to the definition of 'exploitable vulnerability' in Art. 3(38a), clarifying it includes vulnerabilities that have 'the potential to be effectively used by an adversary under practical operational conditions.' The new recital should also state that **the mere existence of a known vulnerability in a product without a possibility of use by an adversary under practical operational conditions does not cause non-compliance.**

We welcome the flexibility introduced in **Annex I(2)(8)** by the Parliament to agree otherwise between the parties in a business-to-business (B2B) context. This reflects that a B2B security patch will require significant efforts between different suppliers, integrators and operators of critical infrastructure, typically planned with functional upgrades whilst ensuring continued availability of B2B systems, and that separation between patches and functionality is not always desirable or possible.

Relationship with RED delegated act

[23] Cybersecurity and Infrastructure Security Agency (CISA), Known Exploited Vulnerabilities Catalog, available at https://www.cisa.gov/known-exploited-vulnerabilities-catalog.

[24] Most vulnerabilities in products are from third-party components, and the biggest job is getting companies to act on vulnerabilities that present a significant risk. As of November 2022, 21,600 new vulnerabilities were recorded in NIST's National Vulnerability Database in 2022, and the total number of listed common vulnerabilities and exposures (CVEs) is about to cross the 200,000 mark. This approach has already been adopted in the US with CISA's Known Exploited Vulnerability Catalog, and we urge ENISA to coordinate closely with CISA in the establishment and maintenance of its own catalogue.

In addition to its relationship with certification schemes, the final CRA text should also more clearly establish its relationship with other applicable EU legislation, and crucially with the RED.[25]

We **support ITRE's clarification under Art.55(3a), allowing manufacturers to comply with the CRA requirements on a voluntary basis** prior to the date of applicability and be considered also to comply with the RED delegated act. We also **strongly support the language clarifying that the Commission will repeal the Delegated Regulation** on the same date of application of this Regulation.

Furthermore, whilst Recital 15 promises that the Commission should 'take into account' the standardisation work carried out pursuant to the RED delegated act's standardisation request,[26] we urge that this should be reflected in an operative provision under Chapter VIII.

Application

Both co-legislators have proposed a transition period of 36 months in Art. 57. DIGITALEUROPE insists that this timeline is too short, and urges that **the implementation period should be extended to 48 months.**

Firstly, given the CRA's wide scope, it is likely that many product groups **won't have harmonised standards available**. This is relevant for products for which self-assessment against harmonised standards will be possible, and also for critical products which must undergo third-party assessment. Notified bodies are dependent on harmonised standards, too.

Secondly, both notified bodies and enforcement authorities are **highly unlikely to have sufficient resources available, nor processes in place**, within the transition timeframe. They need a ramp-up phase to recruit sufficient staff and adapt to new CRA methodologies.

Both aspects are likely to cause a bottleneck with notified bodies, leading to delays of time to market, increased cost and disruption of supply chains.

For tangible products, platform and architecture decisions are made many years before a product is finally placed on the market. In preparing to place products on the market, manufacturers need clear predictable requirements to plan, design, develop and prepare conformity assessment materials. Such predictable requirements are **only available when the relevant harmonised standards are published**. Alternative approaches, such as common specifications or certification schemes, would not necessarily be quicker, and might add to manufacturers' confusion and uncertainty if developed in parallel to potential harmonised standards.

[25] Directive 2014/53/EU.

[26] C(2022) 5637 final.

Finally, by introducing components in the scope of the CRA, an extra delay is introduced for equipment manufacturers incorporating components in finished products. They can only carry out conformity assessment and prepare technical documentation after the completion of the conformity process of the components, and by consequence need sufficient time.

Reporting obligations

Both Council and Parliament have maintained the Commission's proposal for a separate timeline for reporting obligations under Art. 57, proposing 24 and 18 months, respectively.

This separation ignores the inherent compliance link between the CRA's essential requirements and incident/vulnerability handling processes. Making reporting obligations applicable before the rest of the CRA is in place will expose manufacturers to unrealistic, retroactive expectations of compliance they will be unable to meet.

For these reasons, **the part of Art. 57 referring to Art. 11 should be deleted**.

FOR MORE INFORMATION, PLEASE CONTACT:

Zoey Stambolliu

Senior Manager for Infrastructure and Security Policy

zoey.stambolliu@digitaleurope.org / +32 498 88 63 05

Alberto Di Felice

Director for Infrastructure, Privacy and Security Policy

alberto.difelice@digitaleurope.org / +32 471 99 34 25

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, as well as international policies that have an impact on Europe's digital economy. Our membership represents over 45,000 businesses who operate and invest in Europe. It includes 102 corporations which are global leaders in their field of activity, as well as 41 national trade associations from across Europe.

DIGITALEUROPE Membership

Corporate Members

Accenture, Airbus, Applied Materials, Amazon, AMD, Apple, Arçelik, Arm, Assent, Autodesk, Avery Dennison, Banco Santander, Bayer, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, CaixaBank, Cisco, CyberArk, Danfoss, Dassault Systèmes, DATEV, Dell, Eaton, Epson, Ericsson, ESET, EY, Fujitsu, GlaxoSmithKline, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, Honeywell, HP Inc., Huawei, ING, Intel, Johnson & Johnson, Johnson Controls International, Konica Minolta, Kry, Kyocera, Lenovo, Lexmark, LG Electronics, Mastercard, Meta, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe, NEC, Nemetschek, NetApp, Nintendo, Nokia, Nvidia Ltd., Oki, OPPO, Oracle, Palo Alto Networks, Panasonic Europe, Pearson, Philips, Pioneer, Qualcomm, Red Hat, RELX, ResMed, Ricoh, Roche, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Skillsoft, Sky CP, Sony, Sopra Steria, Swatch Group, Technicolor, Texas Instruments, TikTok, Toshiba, TP Vision, UnitedHealth Group, Visa, Vivo, VMware, Waymo, Workday, Xerox, Xiaomi, Zoom.

National Trade Associations

Austria: IOÖ
Belgium: AGORIA
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Czech Republic: AAVIT
Denmark: DI Digital, IT BRANCHEN, Dansk Erhverv
Estonia: ITL
Finland: TIF
France: AFNUM, SECIMAVI, numeum
Germany: bitkom, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: Technology Ireland
Italy: Anitec-Assinform
Lithuania: Infobalt
Luxembourg: APSI
Moldova: ATIC
Netherlands: NLdigital, FIAR
Norway: Abelia
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS
Slovakia: ITAS
Slovenia: ICT Association of Slovenia at CCIS
Spain: Adigital, AMETIC
Sweden: TechSverige, Teknikföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT Ukraine
United Kingdom: techUK