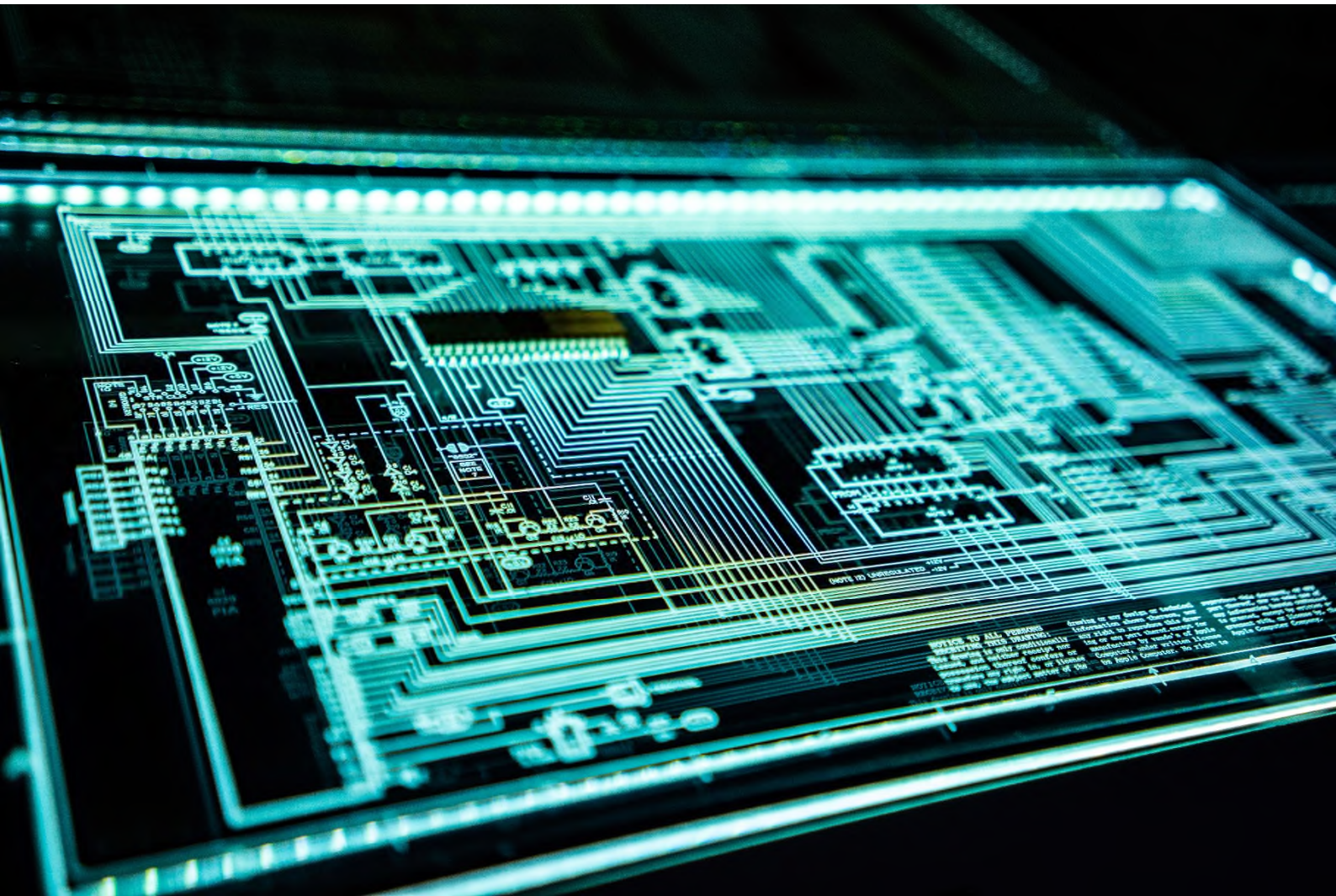
TÜV VERBAND

December 2022

Position Paper

EU Commission proposal for a Cyber Resilience Act

COM (2022) 142 final



Position Paper

EU Commission proposal for a Cyber Resilience Act

The TÜV Association welcomes the European Commission's intention of establishing binding cybersecurity requirements for a broad range of connected products with digital elements. Given the ever-increasing number of cybersecurity incidents across the Union, it is of paramount importance to provide consumers and businesses with secure products both at the time of purchase and over their entire lifecycle. The Cyber Resilience Act (CRA) proposal is a starting point but needs further strengthening on a number of issues, in particular with regard to a coherent and stringent implementation of the risk-based approach and corresponding conformity assessment procedures.

To date, the European Union is lacking an all-encompassing approach to cybersecurity. Cybersecurity provisions in current legislation are limited to specific product groups, incomplete or only applicable on a voluntary basis. Tackling the lack of an overall binding EU-cybersecurity framework, the TÜV Association would have welcomed if the European legislator had made use of the existing Cybersecurity Act (CSA)[1] framework by making its schemes, together with their associated assurance levels and conformity assessment procedures binding[2]. Instead, the European legislator opted for a new horizontal policy framework that, similar to the CSA, does not only cover tangible digital products such as connected devices, but also non-tangible digital products such as software products embedded into connected devices.

The TÜV Association welcomes that all products under the scope of the CRA will have to comply with the proposed cybersecurity requirements, irrespective of their risk level. Thus, all manufacturers will be obliged to take appropriate cybersecurity measures before placing their products on the market as well as during their products' lifecycle.

Apart from setting out ambitious cybersecurity requirements, it is crucial to ensure their consistent and effective compliance. The European legislator has rightly chosen a risk-based approach: The higher the risk level of a product, the more stringent the applicable conformity assessment procedures. However, the proposal falls short of implementing the risk-based approach consistently and coherently. Substantial improvements are needed concerning the risk categorization, the chosen conformity assessment procedures as well as their interplay with sectoral product legislation. The following sections lay down the main areas for improvement and formulate policy recommendations.

[1] (EU) 2019/881
[2] See the two Expert Opinions by Professor Gerald Spindler (University of Göttingen) on the Compatibility of the Cybersecurity Act and the New Legislative Framework

Central demands

1. **Stipulate an independent conformity assessment for all critical products**
   - The distinction between critical products class I and class II is not justified. All high-risk products must be required to undergo a mandatory third-party assessment.
   - Class I and class II products should be merged into a uniform list of critical products within Annex III and be subject to an independent conformity assessment.
2. **Expand the list of critical products to include, amongst others, consumer products**
   - Annex III covers mostly products for industrial use and critical infrastructure but leaves out other products that equally present a cybersecurity risk.
   - All consumer products capable of processing privacy-relevant data, in particular audio-visual data, should be included in the list of critical products in Annex III.
3. **Require the application of harmonised standards to non-critical products for a presumption of conformity**
   - In contrast to existing Union legislation, the proposal does not require the full application of harmonised standards for a presumption of conformity to take effect for non-critical products.
   - The presumption of conformity and thus the use of self-assessment for non-critical products should be restricted to the full application of harmonised standards. Otherwise, a notified body shall be involved.
4. **Ensure coherence with conformity assessment procedures in sectoral product legislation**
   - The conformity assessment procedures for safety and for security aspects must be aligned, as security gaps can compromise the safety of a product.
   - The mandatory assessment by notified bodies for safety-related requirements of sectoral legislation should be expanded to the respective cybersecurity requirements of products.
5. **Ensure coherence with cybersecurity provisions of sectoral product legislation**
   - The conformity assessment procedures of the CRA and of sectoral product legislation with regard to cybersecurity aspects must be aligned.
   - In case of divergences, the more stringent conformity assessment procedure shall apply. This relates in particular to the interplay with the upcoming Machinery Products Regulation.

1. Stipulate an independent conformity assessment for all critical products

The Commission proposal aims to adopt a risk-based approach by distinguishing between de-facto three risk categories. While all products would need to fulfil the essential cybersecurity requirements of Annex I, their applicable conformity assessment procedure differs. Low-risk ('baseline') products would be able to be placed on the market through a self-assessment by the manufacturer without the need to apply harmonised standards. High-risk products ("critical products") are split into two categories: For class I products, a self-assessment is equally possible if harmonised standards are fully applied, otherwise the involvement of a notified body is required. Critical products class II always require the involvement of a notified body.

In the view of the TÜV Association, this approach falls short of implementing the risk-based approach coherently. As a guiding principle, whenever a digital product poses a substantial risk to the user's life, limb, health, privacy, informational self-determination or other fundamental rights, it must be categorized as high-risk and undergo a conformity assessment by notified bodies. As the Commission rightly states in Article 3(3), critical products with digital elements "(...) present a cybersecurity risk in accordance with the criteria laid down in Article 6(2) (...)". It is therefore incomprehensible that the manufacturer would be allowed to place a large part of these critical products on the market through a mere self-declaration of conformity. In practice, critical products such as routers, password managers and industrial control systems would be put on the same level as low-risk products, even though their bear a high risk potential for life and limb. Given the constantly evolving cybersecurity threat landscape, the European legislator should not be solely relying on the mere self-declaration by manufacturers, but should ensure a consistently high level of protection through assessments by notified bodies.

This need is further highlighted by the fact that the distinction between class I and class II products appears to be rather arbitrary. Although the Commission suggests in Recital 26 that a "potential cyber incident involving products in class II might lead to greater negative impacts than an incident involving products in class I, for instance due to the nature of their cybersecurity-related function or intended use in sensitive environments", the CRA proposal does not contain any evidence-based classification criteria or guiding principle that underline these assumptions. It remains therefore open (and questionable) why, for example, class II smartcards are considered to bear higher cybersecurity risks than class I identity management systems software. Likewise, also industrial automation and control systems (IACS) used in non-critical infrastructures, merely classified as class I, could equally entail significant security and safety risks. A hacker with access to the control system of a lift, for example, could take full control over the lift's operation and maliciously change the stopping position of the lift and/or deactivate the emergency button, thus leading to significant safety hazards.

The TÜV Association therefore suggests merging class I and II products into a uniform list of critical products within Annex III and establishing an independent assessment by notified bodies (modules B+C and H) as the sole conformity assessment procedures in line with Article 24(3). This approach would be coherent to existing sectoral EU product legislation within the New Legislative Framework (e.g. the

Medical Devices Regulation), where products classified as high-risk do always require the involvement of a notified body. It would furthermore lead to more stringent and detailed conformity assessments and as a result to a higher overall safety level of digital products in the market.

2. Expand the list of critical products to include, amongst others, consumer products

The criteria for classifying products within Annex III are established in Article 6(2). Amongst others, they comprise that the cybersecurity-related functionality have direct or privileged access to networking or computing resources or control access to data, the intended use in sensitive environments or of performing critical or sensitive functions, and the extent to which the use of products has already caused material or non-material loss or disruption.

While this risk definition appears to be comprehensive, the actual products listed in Annex III are highly selective and only represent a part of the security-critical products on the market. It becomes evident that the Commission considers mainly products intended for industrial use and for critical infrastructure as high-risk, such as Industrial Automation & Control Systems (IACS), microprocessors or secure elements. Consumer products are limited to operating systems for servers, desktops and mobile devices, and Internet-connected modems and switches, with the latter only being included in class I.

The TÜV Association does not share the view that security-critical products are merely limited to industrial applications. Digital products intended for consumers can equally present a cybersecurity risk as they are equally being used in sensitive environments, perform critical or sensitive functions or have caused material or non-material loss. Examples of such consumer IoT products that would be classified as low-risk according to the CRA proposal include smart home appliances such as digital door locks and smart TVs, personal fitness devices or smart toys. Numerous evidence of security-failures by consumer products causing cybersecurity risks[3] [4] illustrate their risk potential.

On these grounds, the list of critical products should be expanded to accommodate all consumer products capable of processing privacy-relevant data, in particular audio-visual data.

3. Require the application of harmonised standards to non-critical products for a presumption of conformity

The large majority of products – 90% according to Commission estimates – belongs to the non-critical, baseline category. While these products do equally need to comply with the essential cybersecurity requirements of Annex I, the Commission proposal does not require the full application of harmonised standards for a presumption of conformity to take effect. Thus, the manufacturer is not obliged to use

[3] In August 2022, the German national security agency BSI issued an official warning not to use an ABUS digital door locks as its radio connection can hacked.
[4] In December 2016, research by the Norwegian Consumer Council revealed that the internet-connected toys 'My Friend Cayla' and 'i-Que' failed basic consumer, security, and privacy rights.

harmonised standards or other technical specifications to demonstrate compliance with the essential cybersecurity requirements in order to be able to use a self-declaration of conformity. Instead, the Commission proposal foresees the unconditional use of the self-declaration of conformity for low-risk products.

This approach stands in sharp contrast to the existing regulatory approach used in EU product legislation[5]. Whilst the application of harmonised standards is always voluntary, it gives rise to a "presumption of conformity" with the essential health and safety requirements of the respective legislation. If harmonised standards are not applied, a notified body has to be mandatorily involved in many cases.

As regards the presumption of conformity with cybersecurity provisions, this regulatory approach has been maintained in existing sector-specific legislation. The Radio Equipment Directive (RED)[6], together with its Delegated Regulation[7], establishes specific cybersecurity provisions for a variety of consumer products. If the manufacturer has not fully applied harmonised standards that specify the essential cybersecurity requirements, the RED requires an independent assessment by notified bodies for the product. If the manufacturer has produced his product in full accordance with harmonised standards, the product is presumed to be in compliance with the essential cybersecurity requirements of the RED. In this case, the additional involvement of a notified body is not needed.

Given the regulatory overlap between the RED and the CRA, the Commission suggests to repeal or amend the RED Delegated Regulation with respect to the radio equipment covered by the CRA, so that the CRA requirements apply only[8]. However, while the Commission points out that the essential cybersecurity requirements of the RED are all covered by the CRA requirements, it does not consider the differences with respect to the applicable conformity assessment procedures, in particular regarding the non-critical product category. Whereas the RED allows a self-assessment (Module A) only if harmonised standards have been fully applied, the CRA allows a self-assessment for "baseline" products in any case regardless of whether harmonised standards have been fully applied or not. In consequence, the repeal of the RED provisions in favour of the CRA provisions would effectively result in the elimination of the mandatory third-party assessment for many consumer products.

In order to avoid a watering-down of the applicable conformity assessment, the European legislators should condition the application of Module A for low-risk products on the full application of harmonised standards. If harmonised standards are not fully applied, the manufacturer should be required to involve a notified body. As a minimum, a conflict-of-law rule should be included according to which products falling under the RED and categorized as non-critical under the CRA should be required to involve a notified body if harmonised standards covering the essential cybersecurity requirements of the CRA have not been fully applied.

[5] This approach is being followed in most NLF legislation, including the Radio Equipment Directive (2014/35/EU) and the Machinery Directive (2006/42/EC), and explained in the Blue Guide on the implementation of EU product rules (2022/C 247/01)
[6] 2014/35/EU
[7] (EU) 2022/30
[8] See COM(2022) 454 final, section "interplay with other Union policies", p. 3

4. Ensure coherence with conformity assessment procedures in sectoral product legislation

The Cyber Resilience Act as a horizontal framework will also directly apply to most sector-specific EU harmonisation directives and regulations as part of the New Legislative Framework[9]. In contrast to the CRA, sectoral legislation is mainly regulating product safety characteristics (i.e. mechanical, electrical and chemical safety) and for the most part does not (yet) cover cybersecurity aspects. That is why the cybersecurity provisions of the CRA will act in addition and complementary to the functional safety provisions of sectoral product legislation.

In this context, it is important to highlight that safety and security aspects cannot be viewed in isolation but are closely interlinked. A security gap may not only compromise a user's privacy or data protection, but may directly compromise the safety of the respective product. To give two examples: A hacker with access to the control system of a lift could take full control over the lift's operation and maliciously change the stopping position of the lift and/or deactivate the emergency button. Likewise, a hacker with access to control system of a cableway could maliciously change the parameters for overspeed or clamping force, leading to a derailment or, in the worst case, to a crash of the cableway.

As a consequence, it is not only crucial to ensure high safety and security requirements, but also regulatory alignment when it comes to the applicable conformity assessment procedures. The CRA proposal does not pay sufficient attention to this crucial interplay between safety and security, in particular with regard to the applicable conformity assessment procedures. To continue with the example, while the Lifts Directive requires the involvement of a notified body to assess all safety components, these components would be classified as critical products class I (Industrial Automation & Control Systems) under the CRA, and thus be subject to self-assessment. As a result, notified bodies under the Lifts Directive would only be eligible to assess the safety characteristics of a lift, but would not be eligible to assess whether the manufacturer has taken sufficient security protection measures for the lift. The same would apply to other products subject to an independent third-party assessment under sectoral legislation, for instance pressure equipment or cableways. Clearly, these inconsistencies lead to a significant reduction of the overall safety and security level and must be avoided.

Addressing these inconsistencies, the TÜV Association suggests incorporating a general clause according to which the mandatory third-party assessment for safety-related requirements as stipulated by sectoral EU harmonisation legislation is directly being expanded to the applicable cybersecurity requirements of Annex I CRA. This general clause would apply independently from the list of high-risk products of Annex III to all EU product legislation mandating the involvement of a notified body[10]. This approach would establish an adequate level of protection and give manufacturers and notified bodies legal clarity.

[9] With the exception of the Medical Devices Regulation (EU) 2017/745 and the in-vitro Diagnostics Regulation (EU) 2017/746, which are both excluded from the scope of the CRA.
[10] This would mainly apply to the Lifts Directive (2014/33/EU), the Cableways Regulation (EU) 2016/424 and the Pressure Equipment Directive (2014/68/EU).

5. Ensure coherence with cybersecurity provisions of sectoral product legislation

As previously mentioned, the aspect of cybersecurity is already regulated within a few sectoral EU product regulations. The CRA proposal includes several articles that address the interplay with the General Product Safety Regulation (Article 7), the AI Act (Article 8) and the Machinery Products Regulation (Article 9). The articles individually lay down how the horizontal CRA requirements relate to the sectoral cybersecurity provisions of the three regulations. The common regulatory approach of these articles mentioned above is that the CRA requirements can be applied to demonstrate compliance with the sectoral cybersecurity requirements. This solution appears to be sensible as such given the horizontal character of the CRA.

However, caution is advised to safeguard an adequate level of protection. On the one hand, it must be ensured that the scope and depth of the respective cybersecurity requirements are comparable to each other before their equivalence can be assumed. On the other hand, it must be ensured that the respective conformity assessment procedures are equivalent. If they are not equivalent, the more stringent procedure must apply. As for high-risk AI systems, the Commission has been carefully following these principles by mandating the stricter conformity assessment procedure for high-risk AI systems according to Article 8(3) of the AI Act proposal.

As for machinery products, though, Article 9 does not explicitly address the applicable conformity assessment procedure but refers to the possibility to use a CRA declaration of conformity to demonstrate compliance with the cybersecurity provisions of the Machinery Products Regulation. Given that most digital elements of high-risk machines would be classified as non-critical or at most class I under the CRA proposal, the manufacturer would be allowed to place them on the market through self-assessment with respect to the cybersecurity provisions on the basis of the CRA. This stands in contrast to the applicable requirements for high-risk machinery products in the Machinery Products Regulation, which mandate an independent assessment by notified bodies for both safety and security. In other words, the manufacturer would be given the opportunity to circumvent a mandatory third-party cybersecurity assessment for the digital elements of his machines by applying the CRA requirements using Module A (self-assessment). As outlined in the previous paragraph, notified bodies would then only be eligible to assess the safety aspects according to the Machinery Regulation, but they would not be eligible to assess the cybersecurity requirements for the digital elements of the machines.

To avoid these inconsistencies, the TÜV Association proposes to clearly specify in Article 9 that critical products with digital elements listed in Annex III of the CRA Regulation, which are also classified as high-risk machinery products according to Annex I of the Machinery Products Regulation, shall be subject to the conformity assessment procedures as required by the Machinery Products Regulation.

Authors and contact

Johannes Kröhnert
Head of Brussels Office
Email: johannes.kroehnert@tuev-verband.de
Tel.: +32 471 79 33 00 | +49 30 760095 500
www.tuev-verband.de/en

Marc Fliehe
Director of Digitalisation and Cybersecurity
Email: marc.fliehe@tuev-verband.de
Tel.: +49 30 760095 460
www.tuev-verband.de/en

The TÜV Association represents the policy and technical interests of its members within the spheres of politics, administration and industry, and vis-à-vis the general public. It is committed to technical and digital safety for products, systems and services through independent assessments and qualified training. The TÜV Association strives with its members to maintain the high level of technical safety in our society and to build trust in the digital world.

Publisher
TÜV-Verband e. V.
Friedrichstraße 136
10117 Berlin

Tel: +49 30 760095-400
Email: berlin@tuev-verband.de
www.tuev-verband.de/en