EUROPEAN CYBER SECURITY ORGANISATION

Challenges of the industry to implement the CRA

WG1 – Trusted supply chains

February 2024

About ECSO

The European Cyber Security Organisation (ECSO) is a non-for-profit organisation, established in 2016. ECSO gathers more than 270 direct Members, including large companies, SMEs and start-ups, research centres, universities, end-users, operators, associations and national administrations. ECSO works with its Members and Partners to develop a competitive European cybersecurity ecosystem providing trusted cybersecurity solutions and advancing Europe's cybersecurity posture and its technological independence. More information about ECSO and its work can be found at www.ecs-org.eu.

Contact

For queries in relation to this document, please use wg1_secretariat@ecs-org.eu.
For media enquiries about this document, please use media@ecs-org.eu.

Disclaimer

Copyright Notice

Executive summary

This document presents the results of a survey conducted with ECSO members to identify potential challenges linked to the implementation of the Cyber Resilient Act (CRA). The survey was conducted in Fall 2023 and it was based on the European Commission proposal text. At the time of publishing, however, a different text following the interinstitutional negotiations has been agreed. Nonetheless, the findings of this survey are still relevant, in that the main priorities and challenges identified remain current.

The outcome of the questionnaire conducted by ECSO, pointed to the lack of clarity with product categories to be the most urgent challenge that organisations are facing when it comes to be in conformance with the CRA. Other relevant and interconnected challenges are the proposed timeline for implementation and the clarity for conducting risk and conformity assessment.

The respondents came mostly from large organisations, for the majority security service providers and manufacturers. Such organisations have quite a good knowledge of industry standards and they employ a significant number of employees working on the security of digital products. In light of this expertise, most of them estimated that they will be affected by the CRA, and they were also able to estimate the expected costs in money and the time required to be compliant to the CRA. The limited engagement from SMEs observed in the survey could stem from a lack of engagement or understanding of the CRA and its implications could be a starting point for further initiatives.

Even though the answers where highly articulated, in term of asks to the EU, it emerged the need for guidelines and templates, training on compliance, and the availability of automated vulnerability and risk assessment tools. Any early adopter example would be welcome.

Table of Contents

1 Introduction

1.1 Context

The purpose of the initiative is to identify potential challenges that ECSO members foresee or might arise from the **implementation of the Cyber Resilience Act (CRA).** This will contribute to have a better understanding of the potential impact for the market**.**

This document is the result of the survey stemming from the exchanges ECSO has had with the European Commission and also builds on previous initiatives, such as webinars held by ECSO on the CRA. The survey was based on the European Commission proposal text[1], while at the time of publishing a different text following the interinstitutional negotiations has been agreed. Nonetheless, the conclusion of this survey is still current to understand the impact of the CRA for the market.

Ultimately, the purpose is to support the European Commission with the view of the ECSO members about what needs to be done to prepare for the deployment of the CRA and ensure a smooth process for the organisations that need to comply with the regulation.

The results are also instrumental in defining the work items of the ECSO WG1 on Trusted Supply Chain for the future. The objective is to work on concrete outcomes that could support and facilitate the implementation of the CRA as well as **empowering organisations with the right tools and guidelines the market will need for such implementation**.

As such, this exercise was aimed at the technical aspects of the implementation of the CRA, not the policy itself.

CRA Information

The Cyber Resilience Act (CRA) was proposed by the European Commission on 21 September 2022[1].

The objective of the CRA is to establish a minimum level of cybersecurity for all digital devices (both software and hardware) sold in the EU internal market. It is expected that with the CRA, manufacturers of digital devices and services will be required to provide security updates and remediation of vulnerabilities throughout the product life cycle or a support period.

The most significant impact is expected to fall on IoT products, both for home and industrial applications, with a low level of security or limited ability to receive updates to heal vulnerabilities. There will also be a significant impact on network infrastructure hardware products and opensource software for sale. It will also try to solve the problem of supply chain security. The most

[1] European Commission. Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020. COM(2022) 454 final. September 2022.

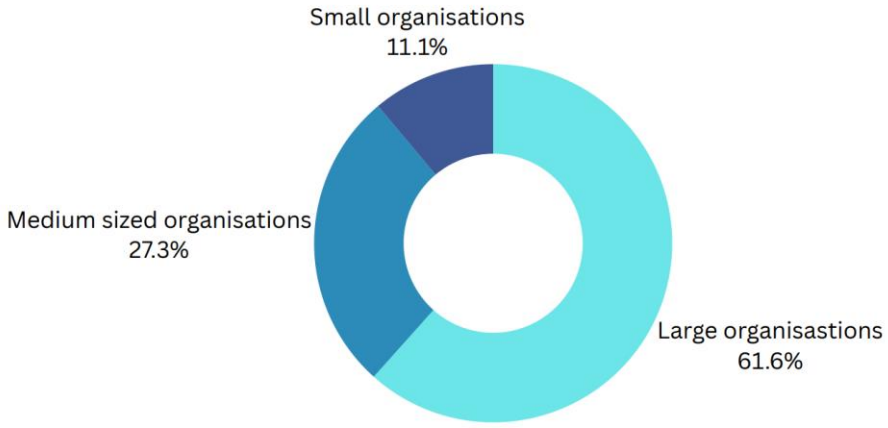
sophisticated cyber-attacks in recent years have in fact targeted software and hardware components that were then used by many companies downstream in the supply chain.

More information about the Cyber Resilience Act is available on the Legislative Observatory of the European Parliament[2].

1.2 Questionnaire methodology and structure

The respondent to the questionnaire were a sub-set of ECSO members, representing for the majority Security service providers and manufacturers, even though other public and private organizations participated.

61% of the respondent were large organization (with more than 250 employees), whereas 27% were medium size (between 50 and 250) and 11% small (less than 50 employees).



33% of the respondents reported to employ more than 100 employees in their organization dealing with the security of their products (so not simply “security aware” personnel).

A note about SMEs

Despite the questionnaire being share to SMEs, only a minority of the respondents represented this category. This in itself is an interesting finding giving that SMEs are a fragile target to cyber-attacks and cyber related issues. A recent report from National Cyber Security Alliance of the US showed that 60% of small companies go out of business withing 6 months after a breach, and this could be an indication to European businesses. Therefore, such finding would call for further inquiries into why there seems to be a lack of interest (or understanding) of the CRA by the backbone of the EU industrial infrastructure.

[2] https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2022/0272(COD)&l=en

2 Challenges and priorities

The questionnaire proposed a number of potential challenges related to the implementation of the CRA and guided the respondent in selecting the most pressing ones. It emerged that **Clarity with product categories** was the top priority among the choices. The selection item read, in particular, *Clarity with product categories with regard the difficulty to understand with legal certainty in which category a product falls in.* Obviously, the challenges proposed (see the list below) are all interconnected, and in many cases dependent on each other. As a consequence, participants had the chance to comment on and select all the others as well.

List of proposed challenges:

2.1 What is my product class?

The clarity with the product categories was, overall, the most recurring concern, one that is perceived essential in order to be operational on the market and perform all the other related procedures required by the CRA (i.e. risk assessment, conformity assessment etc…). As previously mentioned, the survey was based on the European Commission proposal text, different than the text following the interinstitutional negotiations available at the time of publishing of this survey. In this case, the product categories are different from the ones highlighted in this survey as currently the distinction is made among: Product with digital elements, Important products Class I and II, Critical Products. Nonetheless, the conclusion of this survey is still current, in that organisations need support in understanding with certainty what category one products falls in.

The demand of the participants to the survey is for a clearer demarcation between product lines, **with a clear product taxonomy**. In addition, even if it was up to organisation to identify categories, the methodology to be used is not clear either.

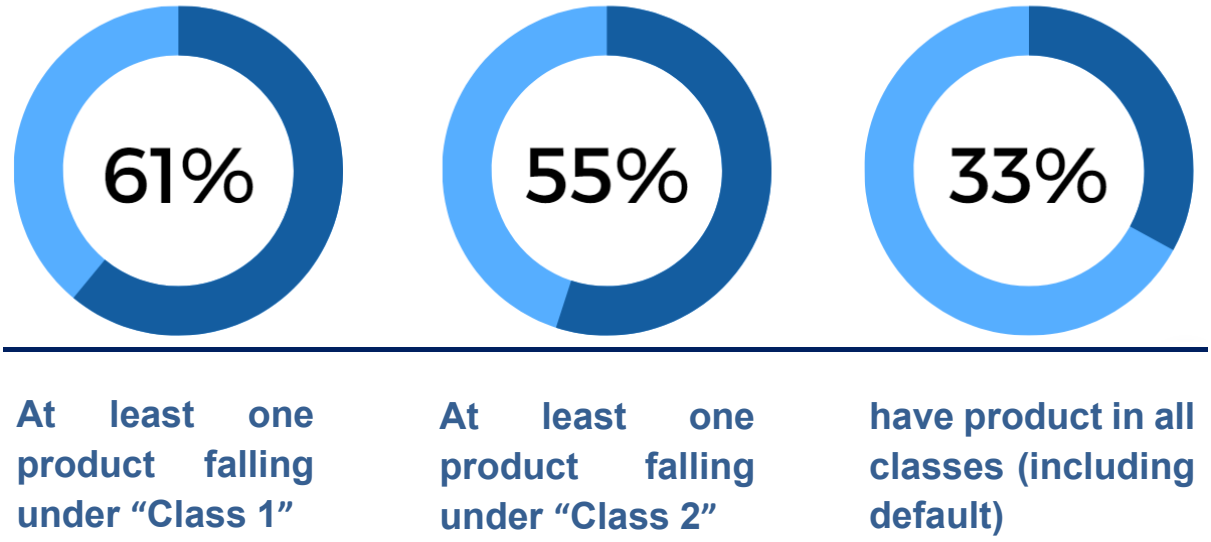
Moreover, the concept of “functionalities” and “intended use” add some complexity as many products could fall under different categories. Such categories will depend on the intention of the customer, or end-user in general, so that the product in question might end up being used within risk areas not previously foreseen by the vendor.

More in general, clarification at more granular level will be useful, especially when it comes to specific concepts, such as “*negative impact of the exploitation*” (recital 25) or specific category distinction, like IoT vs IIoT products for instance. Following this reasoning, for many vendors it is crucial to understand what products are “critical”, given that they are often already complying with existing stringent rules; some respondents also fear that an extended definition of “critical product” would virtually include most products with digital elements, shifting the focus of the CRA from the essential requirements and baseline standards to the products for which manufacturers already invest significant resources to ensure security.

From a market perspective, stability and clarity of product categories would help prevent the risk of unfair labelling among competitors as well as facilitate the implementation of and investment in the right processes. Finally, the urgency of clear product class definition stems as well from the need to clarify the interplay with other regulations, standards and certification schemes (such as CSA, EUCC, etc…).

2.1.1Products in your organizations impacted by the CRA

Despite all the considerations above, respondents were still able to estimate the type of product of their organisation that would be impacted by the CRA. In particular they reported to have:



2.2 Timeline

Given the targeted timeline from the EC[3], many respondents highlighted it as a challenge, with three perspectives emerging:

From an ecosystem point of view, **several standards and certifications will need to be developed** and made available in the upcoming years. **CABs risk to be overloaded** and will need time to adapt.

From a market perspective, not all the **players will have the same knowledge about the CRA nor they will be up to speed with the current and planned developments** as the dissemination of the information will take time. In addition, companies (as well as CABs) might be delayed in finding the **skilled professionals**. Finally, some organizations will have to deal with their structural complexity (larger portfolio, subsidiaries, specific governance structures); on the other end smaller players might simply not have enough resources.

Finally, changes will be challenging for organisations, especially for those with products in class 2 category: **vendors will need to adapt their processes** of development, manufacturing and management. Given the importance of these products for the overall society, enough time should be granted for testing and adapting to these changes.

A final mention about semiconductors providers: vendors and manufactures using semiconductors components will need to have semiconductors providers to be compliant in the first place, in order to be compliant themselves. The time pressure for such provider will be, therefore, even tighter.

2.3 How shall I perform my risk and conformity assessment?

More than half of the participants mentioned the following two main aspects in their responses.

1. The definition of a unified approach and similar tools for conformity assessment can be achieved if more details will be provided. This will also help limiting the scope for individual interpretation.

   One example is providing common guidelines to define how to do a risk assessment to classify the product in the right category or how to proceed when in need to update a risk assessment in light of new vulnerabilities (especially when it comes to 3rd parties).

   Overall, it seems that there is a lack of knowledge on harmonized guidelines and methodologies at EU level. Delays in clarifying this might lead the way to overlapping risk assessment methodologies.

2. Similarly, when it comes to conformity assessment, further clarity would be welcome as a step towards preserving competitiveness of organisations impacted by the CRA.

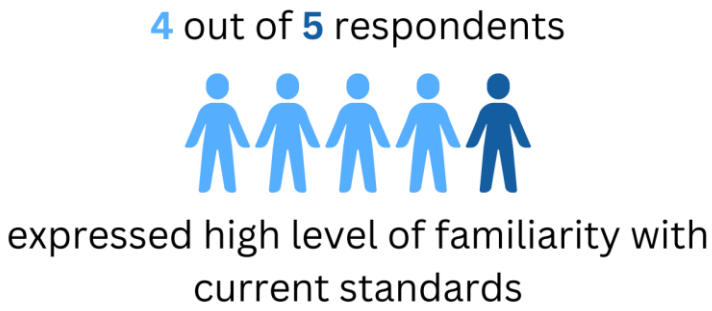
[3] The tentative timeline proposed by the European Commission is 36 months from the entry into force of the CRA.

Increased clarification will be beneficial to conformity assessment providers and CABs as well. The latter will need support on areas such as threat modelling, design review, source code review, security functional testing, penetration testing, etc... All this will help create a level playing field in all member states.

2.4 Yes, but what standards?

A significant portion of the participants focused on the **availability of standards** as well. This applies both for horizontal and vertical standards, whose applicability, readiness, and coverage appear to be only partial at EU level. Obviously, requiring conformity to standards that are not yet existent might lead to confusion. Guidance and examples about existing criteria and standard conformity criteria will be, therefore, more than welcome and possibly a transition period will be beneficial. Even a simple assessment matrix for the sake of users, producers and certifiers would be of help. As mentioned previously, **uneven adoption and availability of standards among Member States is also a concern** and some participants also stressed the importance of **harmonization of standards at European level**.

"ISO/IEC 27001 and IEC 62443 were the most quoted standards in the survey"



The respondent exposed overall quite a high level of familiarity with current standards, both for processes and products (on average 4 on a scale of 5). They quoted several standards in their current practice as confirmed by their proficiency. The most quoted standards (by 70% of them) was ISO 27001, followed by the IEC62443 Series.

2.5 Guidelines for manufacturers

Half of the participants selected the challenge of **lack of guidelines for manufacturers**, even though not all participants were manufacturers. Few comments were made about details, such as support **coverage and maturity of product development**, that can matter a lot for manufactures and expand substantially the number of products impacted by the CRA.

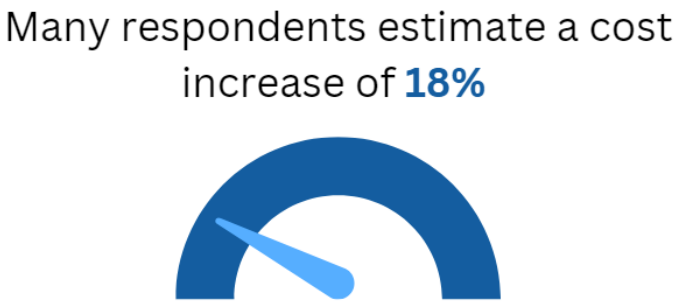
On the other hand, smaller players expressed some concerns too, as having less negotiating power might result in the compliance burden being "pushed" toward them by larger producers.

Another interesting point was raised about the need for guidelines when it comes to products with software licence models (being that on premises or cloud): when talking about lifecycle, it is not yet clear how would that map to the licence model timeframe.

2.6 The costs of regulation

Time and money are part of the cost that suppliers of all sizes have to deal with daily. Therefore, it is important to understand how those aspects are expected to play a role with regard the CRA.

Quite interestingly some of the answers (for the respondents who sells products or services) highlighted the **expectation of a price increase** as a result of the adoption of the CRA. The average estimation was of 18%.



The cost in time, or in other words, the estimated time needed to be compliant with the CRA, was expected to be between 1 and 6 months, for 55% of the respondents. However, it is worth noticing here that this question could have been interpreted slightly differently by respondents: larger companies in particular might have estimated this parameter per product, so that the actual timeframe would become longer if calculated for all the product portfolio.

On other general matters, some respondents highlighted the known questions concerning open-source components and how to conduct assessment in this case. Other challenges could be faced in case of trade secrets when sharing information about product assessment and disclosure more in general. Around 20% of the participants expressed a generic lack of documentation.

3 Support for the implementation of the CRA

This section focuses on the implementation of the CRA and what could help organisations prepare.

In your opinion, what supporting documents do you need to facilitate the CRA implementation?

Most of respondents quoted guidelines, templates, checklist and reference use cases. More in particular, the need for guidelines appears to be one of the greatest: general **guidelines, about product taxonomy and processes**, interpretation **guidelines, for interaction between**

manufacturers and resellers, for producing end-users checklists, for remote data-processing solutions, **accreditation criteria for Certification Body/Notified Body/Evaluation Lab** etc…

With regard templates, we identified the need of **templates for risk and conformity assessment results, the procedure for the assessments and processes in general, templates for self-declaration, for product classification, templates to be used to communicate and disclose security information to the relevant bodies**. In general, such templates should be standardised enough to avoid interpretation and allowing an efficient communication flow among all the stakeholders involved in the CRA implementation.

Respondents also highlight the need for reference use cases for risk and conformity assessment and implementations references.

Finally, we registered answers concerning the need for lists and checklists: list of standards to comply with per product category, list of certification providers, of entity to test, evaluate and certify. Furthermore, checklist to ensure the product lifecycle maturity is optimal, to enable timely reporting for CRA compliance and checklist of rules for implementation for each product category, to enable a compliant go-to-market strategy.

In your opinion, what type of training you or your organization need to facilitate the CRA implementation?

Trainings on compliance assessment was the most chosen answer (both from a technical and legal point of view), followed by **trainings on risk and conformity assessment**; some answers also stated the need for support from a certification expert and training on how to communicate and interact with the relevant authorities (e.g., CERTs, ENISA etc.); training for process changes (especially for vulnerability management).

In your opinion what kind of tools would facilitate and support the CRA implementation?

The number one wish was for **Vulnerability and Risk Assessment (as well as management) tool**, Ideally the automation provided would also help the reporting and possibly reporting directly to the pertinent authorities. Other example quoted were FAQ lists; SBOM automation and validation; Decision making support systems for technology sourcing; compliance and certification verification tool; list of reusable standards; Implementation examples and use cases. Finally, one of the comments expressed also the wish that such tools would not be “mandated”.

What do you think is missing to facilitate the implementation of the CRA?

Some of the comments repeated and detailed more the need for clarity and stability in order to make the CRA smoothly applicable. Guidance is very much needed, and concerns relates to the fact that given the deep scope of the CRA, its application in the intended timeframe will represent a competitive disadvantage for European manufacturer.

It is worth mentioning the wish for **opportunities of learning from early adopters**, possibly having the EC facilitating that.

Overall, there is a wish for increased collaboration between international bodies (such as ISO, IEC, ITU) and European (such as CEN, CENELEC, and ETSI) and national authorities, facilitating a common understanding, with the aim of creating internationally valid standards. Similarly, at European level it would be interesting to understand better the **connection and interplay of the CRA with other EU regulations** both horizonal and vertical (RED, CSA, Machine Directive, NIS2, CSA etc.).

Other points worth mentioning:

- Special care should be provided for national accreditation bodies and their readiness (time, tools, knowledge, etc.).
- A holistic cybersecurity skill strategy linking private and public entities providing education and certification with companies, especially SMEs, required to be CRA compliant.

Other missing points: a legal definition of High-Risk Vendor, clear guidelines on software, complexed structured products, modular products, family of products.

4 Recommendations and key takeaways

Based on this analysis, enriched with interlocks with European stakeholders, ECSO members, and the guidance of the ECSO Working Group on Trusted Supply Chain, some key takeaways have been identified as important aspects to facilitate the CRA implementation for the market.

As it became clear from the analysis, organisations face a number of challenges when it comes to implementing the regulation. Many, SMEs in particular, appear to be lacking an understanding of what the CRA is and if they fall under its scope. In particular, notwithstanding the type of product categories, it is important to help businesses understand what category one products falls in. Once this is established, there is a need to understand what should be done practically to be compliant, how much time do we have and what tools are available.

Furthermore, this analysis, combined with ECSO's expertise, highlighted the need to develop and strengthen a composition approach for conformity assessment focussing on the technical and operational aspects. Despite consensus that such approach is important and it is also recommended by the CRA, it is more complex to apply it in practice, and a clear methodology (building also on previous papers proposed by ECSO) would be useful.

From a practical perspective, the European market will need tangible guidance with regards to certification and conformity to the EU regulation. Some of the solutions identified are: possibility to provide practical workshop and enablement sessions; guidelines and templates, training on compliance, and the availability of automated vulnerability and risk assessment tools with possibility of learning from early adopters. Furthermore, some form of questionnaire and workflow to understand if one is "in scope" of the CRA could be useful, especially for smaller businesses.

Last but not least, a successful implementation will depend as well on the clarity of the overall interplay of the CRA with other EU pieces of law. Anything that will help clarify these intersections will, therefore, be highly beneficial.

ECS
EUROPEAN CYBER SECURITY ORGANISATION

> JOIN ECSO

29, RUE DUCALE - 1000 BRUSSELS - BELGIUM
ECSO IS REGISTERED AT THE EU TRANSPARENCY REGISTRY 684434822646-91
WEBSITE : WWW.ECS-ORG.EU