POSITION PAPER

Brussels, 5 April 2023

Orgalim's position on the Cyber Resilience Act

Executive summary

The pace at which products with digital elements are being developed is truly astounding. Currently, it would be no understatement to say that the number of these types of products can be counted in the millions. They range from automobiles to toys, from industrial to home appliance products, and the list continues to grow. This means that today we can find such products practically anywhere. However, with the proliferation of products with digital elements and digitalisation, the susceptibility to cyber threats by malicious actors also increases.

In order to find a European solution, on 15 September 2022 the European Commission published its Cyber Resilience Act (CRA) proposal which aims to bolster cybersecurity rules for hardware and software products. Orgalim welcomes the Commission's initiative, although we believe that in order to make the Act workable and effective, the following elements should be taken into account:

1. The criteria that determine the criticality of products with digital elements must be clear in order to avoid legal uncertainty. Furthermore, the risk assessment should not only be based on the nature of the product, but also on the potential severity of impacts with regard to the intended use of the product.
2. The CRA should focus on products or product components that can be subject to, or be part of, a malicious cyber threat. Moreover, the term "cyber" should be clearly defined, as this is currently missing.
3. A transition period of 48 months after the entry into force should be given to ensure that the industry is prepared to comply with the provisions laid out by the CRA. The CRA is the first holistic regulation attempt for the cybersecurity of products, therefore every actor from the standardisation bodies to the respective component or product-manufacturers needs adequate time to adapt their products and processes and expand their personnel. This also includes the notified bodies. Alternatively, a staggered approach could be implemented.
4. The text of the CRA should ensure legal certainty with all legislation that also addresses cybersecurity. In particular, the relationship to the Radio Equipment Directive Delegated Act must be established more clearly.
5. The essential requirements laid out in Annex I are currently not precise enough to ensure the legal certainty needed. Moreover, in order to ensure proportionality, the reporting obligations must be limited to 'exploited vulnerabilities with a significant impact' only.
6. The alignment with the New Legislative Framework (NLF) could be further strengthened by using already existing NLF definitions. Harmonised standards should be the primary and preferred way to detail technical requirements.
7. The fines under the Market Surveillance Regulation should apply for products with digital elements covered by the CRA. Additionally, manufacturers should not face penalties when they use components from third party suppliers that are later deemed to have vulnerabilities.

Introduction

On September 15, 2022, the European Commission published its long-awaited "*Proposal for a regulation on horizontal cybersecurity requirements for products with digital elements*" – the EU Cyber Resilience Act (CRA).

As already stated in the Orgalim response to the public consultation, Orgalim welcomes this draft as a major and decisive step towards a cybersecure Europe. We appreciate that the Commission has chosen the New Legislative Framework (NLF) as the basis for the regulation to build on the success of European CE product regulation.

This legislative proposal addresses at the same time both pure software and hardware companies using software in their products. Laying down rules for millions of products in the EU single market, its impact cannot be underestimated. Therefore, specific characteristics of these industries must be sufficiently addressed. For instance, the possible extensive lifespan of industrial products, which can be up to a few decades, and the corresponding legacy will present a challenge for balancing security, management and the repairability of products placed on the market.

In the following sections we have identified seven key aspects of the CRA for which changes should be made. We see such changes as necessary to enhance effectiveness and avoid pitfalls that might be detrimental to European cyber resilience and economic competitiveness.

1. Criticality criteria and product groups

1.1. Article 6(2)

Article 6(2) outlines criteria for the identification of product-specific cybersecurity risks. We would advise to further clarify such criteria and improve the definitions. Concretely, we suggest:

1. To clarify how the two levels of criticality (Class I & II) are differentiated. We would advise to make use of the "intended use" criteria of a product to define the levels of criticality more efficiently. Further clarification could be reached by amending the last sentence of Article 6(2): "*one or several of the following criteria shall be taken into account **in relation to the intended use of the product***".
2. To make criterion 6(2) a) proposed by the Commission cumulative with either 6(2) b), c), d), or e), to allow for a better identification of critical products. Additionally, the categorised products should focus on products in critical applications (for example, an industrial firewall used by an essential entity as per NIS2).
3. To delete 6(2) a) iii as "operational technology" is a term that can be interpreted broadly. The terms need to be precise to clarify the scope. Not every application in Operational Technology (OT) or industrial environment (compare the terms "industrial automation and control systems (IACS)" and "industrial" used in Annex III) is critical.
4. To delete the reference to "industrial settings" in Article 6(2)b). Indeed, while we concur with criticality for intended use by essential entities (according to NIS2) we are convinced that many industrial applications will be sufficiently covered by conformity Module A of Decision 768/2008/EC (New Legislative Framework), because not every use in an industrial setting is critical.
5. To differentiate critical applications (meaning applications that are critical for the business process or product where it is used) from critical environments (meaning environments that are critical for the society or the state at a larger scale). This would allow for a more precise classification concept as we suggest for Annex III below. Therefore, we propose to change the language in Article 6(2) b) from intended use in "sensitive environments" to intended use in "critical applications" [by essential entities …].
6. To ensure that 6(2) e) (materialisation of an adverse impact) is based on factual evidence of the materialisation of a risk, as well as on the criticality of such an impact established through a risk assessment.

1.2. Annex III & Article 6(5)

The core strength of the CRA is its use of the NLF, which ensures a risk-based approach, as legal requirements are set according to a risk assessment which considers the intended use and intended operational environment of a product. This principle should be maintained, and the level of risk should be reflected in the categorisation of critical products under Annex III, Class I and Class II. Therefore, in addition to the nature of a product with digital elements, the "intended use" and the operational environment of the product should also be added as elements for the Class I or Class II categorisation.

As defined in Article 6(2), we would suggest basing the risk assessment not only on the nature of the product but also on the potential severity of impacts of the intended use of the product, to decide on its categorisation level as a critical product under Class I or II.

Further concrete suggestions for Annex III include:

1. Remove routers and switches that are not fulfilling any explicit or implicit firewall functions.
2. Class I, 15: delete physical network interfaces as this would turn any plug for data connection into a critical product and replace it with "physical network interfaces to public networks".
3. Recategorise Class I 22 & 23 and Class II 12 & 13, and add the following criteria:
    a. (Common) IACS and IIoT Products are generally non-critical ("Class zero") because they are used in a non-critical application
    b. IACS and IIoT Products Class I: Products intended by the manufacturer to be used in critical applications at NIS2 important entities
    c. IACS and IIoT Products Class II: Products intended by the manufacturer to be used in critical applications at NIS2 essential entities
4. Consider including Enterprise Resource Planning software as critical, given that such software is clearly a critical function for all (NIS2) important and essential entities.
5. Recategorise Class II 14, and move it into Class I 22, because the risk of this category is already sufficiently covered by the text of the draft Machinery Regulation.
6. Class II 4 & 7, replace the reference to "industrial" use by "intended for use in critical applications in NIS2 essential entities".

Additionally, Orgalim advises caution concerning the introduction of Article 6(5), which allows for the categorisation of a new class of "*highly critical products*", "*for which the manufacturers shall be required to obtain a European cybersecurity certificate under a European cybersecurity certification scheme pursuant to Regulation (EU) 2019/881 […]*". We see the following major issues with this paragraph:

1. The application of mandatory CSA Schemes for highly critical products as the only market access condition is contradictory to the NLF concept that builds on hEN standards for definition of technical details. In any case, the ultimate legal requirements for market access are defined in the product law itself and should not be delegated to a certification scheme coming from another regulation. Moreover, the CRA already calls for mandatory third party involvement for all "critical products" of Class II and the same mandatory third-party involvement could be used for a newly defined category of "highly critical" products.

2. Having the already too broad and unspecific categorisation of critical products in mind (Annex III), the introduction of another category for products, which may stay undefined for an unspecified amount of time, adds additional uncertainty for the industry.

3. Article 18(3) and 18(4) of the CRA already allows for the specification of CSA Schemes, which could be used to show conformity with the essential requirements set out in Annex I. This includes the use as a surrogate of the third party conformity assessment as set out in Article 24(2) a), b), (3) a) and b). Those provisions also match Article 24 (1 & 2)

of the NIS2 directive, which are already sufficient to avoid making the CSA Schemes mandatory for certain highly critical products and which make a double regulation unnecessary.

If the legislator does choose to allow for the option to create a new criticality class, both the definition of such a class and the conformity assessment process need to be more clearly specified. For the reasons listed above, Orgalim asks for the deletion of Article 6(5).

Finally, we support the idea (see recital 27) that the core functionality takes precedence over criticality so that a compliant critical product integrated into a default category product does not automatically make the default category/complete product critical. In addition to the recital, the legal provisions of the CRA could be more explicit. The legal provisions of the CRA should clarify that components referred to in Annex III are categorised only as critical when they are placed on the market separately.

2. The product scope

2.1. General considerations

Article 2(1) states: "*This Regulation applies to products with digital elements whose intended or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network*."

This wording assumes that any digital product capable of exchanging data through a connection is susceptible to cyber threats. This is not proportionate, and the following example illustrates that, as it stands, the current wording applies to products which only pose a negligible risk in regards of security or have a minimal susceptibility to a cyber threat:
A smoke detector, connected only to a fire detection control panel via a bus connection, is exchanging data reflecting the measured amount of smoke, detected fault and other status information. The bus is connecting many detectors and other fire detection components in a loop, and therefore forms an isolated local network entirely managed by the control panel.

In the example, the products in the isolated network behind the control panel should lack the threat exposure, as the panel takes a gateway function, including security functionalities for the products in the isolated network. The risk for any cyberattack on the detector and on any other field electronic device in the loop is minimal, due to their limited capabilities and the protection behind the control panel, acting as a security gateway. The described operational environment would therefore have to be part of the considerations in the respective risk assessments of the connected products and of the control panel under the CRA, meaning the essential requirements of Annex I would have to be assessed accordingly. Similar reasoning is valid for any sensors and other electronic devices which are part of and only communicating with an isolated network behind a security gateway within a product with digital elements in the scope of the Regulation.

Therefore, we urge the legislator to further specify the data connection in Article 2(1), to focus on those products which genuinely are susceptible as the target of a cyber threat; for example, by focusing on products whose intended or reasonably foreseeable use includes a logical or physical bidirectional data connection to a device or network. Moreover, there is a need to clearly define the term "cyber", as it is currently missing, and further clarify "cybersecurity risk", as it now only refers to the definition of the generic term "risk" included in NIS2.

Finally, and as a reminder, under the NLF a component usually only falls in scope once it is placed on the market separately. Otherwise, the component is part of a containing product and is indirectly covered through the conformity requirements of that product. We therefore believe that the limited capabilities of most components, and the question of how components could be correctly addressed in consideration of their incomplete character, should be examined in more detail in the CRA.

The need to comply with the CRA is triggered by "placing on the market". This means that products which are used only by the manufacturing entity (i.e. where there is no onward supply to a different entity), will not trigger the need to comply with the CRA. Therefore, it is our understanding that products that are exclusively produced, supplied and used within the same corporate group of the manufacturing entity would be out of scope.

2.2. Software as a product and remote data processing

With the introduction of software as a product, the CRA may have a much wider scope than intended, with additional uncertainty when it comes to software-based services (e.g. cloud computing) and software as a service (application not running on the user's device). For the Medical Devices Regulation, this issue was addressed by the definition of the specific purpose of the software (i.e. medical use). For the CRA the consideration of "remote data processing" in combination with software as product blurs this line.

Articles 3(1) and 3(2) define "*product with digital elements*" and "*remote data processing*". We understand that the intention is to cover any digital product, but we suggest further clarification of which remote data processing solutions would be part of the CRA and why.

We concur with the Commission (as elaborated in recital 9 and the explanatory notes) that the CRA should not cover services. This is very important as services cannot be placed on the market (as defined in NLF) and are regulated in a different way compared to goods. Cloud service providers falling under the NIS2 would thus not risk undergoing double regulation of their service, while the security of the cloud is ensured by the NIS2. However, when it comes to Software as a Service (SaaS) this differentiation becomes more complicated as SaaS essentially has the same purpose as other software solutions and should therefore meet corresponding security requirements. Additionally, many applications (e.g. a voice assistant) have cloud back-ends running on a massive number of networked servers around the world. Although such a cloud infrastructure is not subject to the CRA, as is described in recital 9, it would be worthwhile to ensure that the definition of remote data processing solutions does not create an unwanted overlap with the NIS2 Directive. Therefore, the definition of remote data processing should be further specified and limited.

2.3. Pre-production software

The CRA also acknowledges that modern software development requires the release of "unfinished software" (also known as "alpha" and "beta" releases) for feedback, testing and "bug discovery" (see recital 21). We believe it should explicitly clarify in the provisions that these products are not within its scope. Importantly, individuals who sign up to be alpha/beta users are sophisticated technology consumers, who understand the software is incomplete and simply want to experience the latest features and steer the product's direction with their feedback. These are not the type of consumers that the CRA intends to protect.

2.4. Spare parts

Especially in the context of industrial products with their long life cycle and legacy, spare parts should be excluded from the scope to ensure the functioning, maintenance and reparability of long-lasting products. Therefore, we suggest excluding spare parts which are used in maintenance operations (in-line with the Blue Guide) of products from the CRA scope. An exclusion would be very limited in its consequences for the resilience level, as spare parts have to be a direct fit; therefore, their use will not change the cyber resilience level of the product or the application in which it is used.

3. Transition periods and application dates

Article 57 of the CRA proposes its entry into application 24 months after the entry into force of the Regulation. Considering that usually standardisation requests are adopted after the publication of a legal act in the Official Journal of the EU (OJEU), this would only allow less than two years for the development of harmonised standards. Given the length of time it would take for the ESOs to develop the harmonised standards, especially considering the uncertainties introduced by articles such as Article 6(3) which could lead to some changes during the standardisation effort, this implies that the standards would be available at the earliest by the time the CRA is applicable. This would leave no time for manufacturers to ensure conformity of their products, especially since it is to be expected that internal processes must be established, adapted, or changed and products may need a re-design to fulfil the new requirements. Furthermore, and for manufacturers to be able to use the harmonised standards, these will also have to be assessed by HAS consultants and published in the OJEU, which adds a further delay. Lastly, it should be considered that notified bodies will also need to be appointed, and this may be difficult considering the fact that only a limited number of notified bodies (currently only four) have knowledge on cybersecurity standards.

As such, Orgalim advocates for a general application time of at least 48 months after the entry into force of the Regulation. A staggered approach could also be considered, meaning the setting of different implementation times for different products. Additionally, the application time of Article 11 – proposed to be 12 months after the date of entry into force – also seems unreasonable. This should be adjusted accordingly, and Orgalim believes Article 11 should also apply after 48 months after the entry into force, or again, potentially with the application of a staggered approach.

4. Relationship to other legislation also addressing cybersecurity

Orgalim supports that compliance with the CRA automatically provides for presumption of conformity with the cybersecurity requirements under the Machinery Regulation and the General Product Safety Regulation. Moreover, we would like to voice our opinion on the legislation below.

4.1. Regulation 2022/30 (RED Delegated Act)

The introduction of the RED DA followed by the CRA is creating significant legal uncertainty for the industry, and the issue has to be clarified as soon as possible by the Commission in order to minimise the delays and costs for industry.

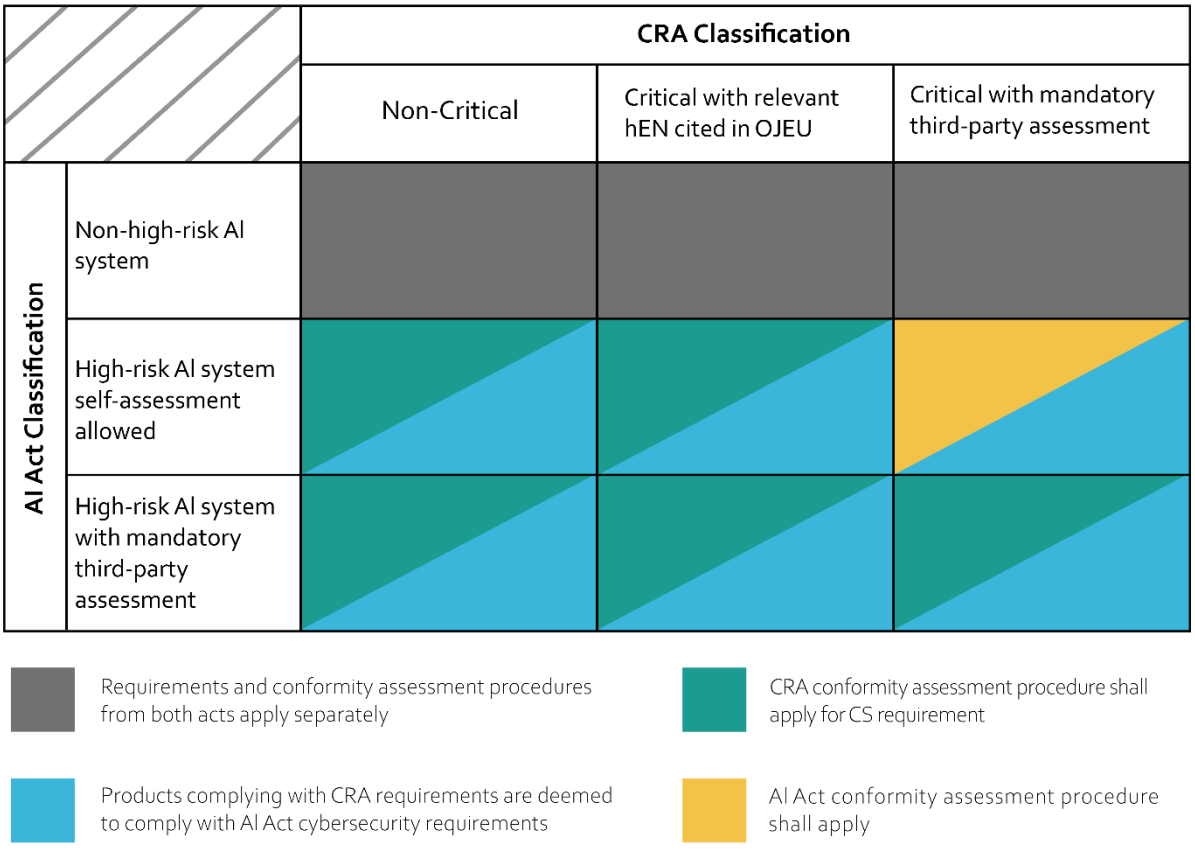
To avoid legal uncertainty for industry, the CRA should be the central reference point for the cybersecurity of products. Double regulation has to be avoided, and transitional provisions for the respective compliance for products under the CRA and Article 3(3) d), e), f) of the RED DA have to be included in the CRA to protect the legal certainty on which the European market thrives. It has to be ensured that the lessons learned and the best practices from the standardisation work on the RED DA Article 3(3) d), e), f) feed into the CRA standardisation work, and the drafting of the CRA itself and its standardisation request.

4.2. Network and Information System Directive (NIS2)

The CRA makes references to the NIS2 Directive on several occasions which Orgalim recognises and encourages. The NIS2 must be seen as complementary to the CRA; while the latter regulates product compliance, the former ensures that relevant entities in the EU meet the cybersecurity requirements for information systems.
However, to avoid any duplication of requirements, Orgalim suggests that special attention should be given to the requirements under NIS2 and the CRA for essential and important entities. It should be further clarified that digital products in the scope of the CRA are not covered by NIS2 and vice versa. Thus, the CRA ought, as suggested, include a clear distinction between its provisions and those of the NIS2.

4.3. Future AI Regulation

Article 8 tries to explain the relationship between the proposed CRA and the cybersecurity provisions of the proposed Regulation on Artificial Intelligence (the AI Act). Our analysis of Article 8 led us to summarise it with the following table:



Assuming this analysis is correct, we understand that non-high-risk AI systems in Article 8 do not benefit from a privilege granted to high-risk AI systems, which is that products complying with CRA requirements are deemed to comply with AI Act cybersecurity requirements.

We therefore recommend that Article 8 should state that non-high-risk AI systems complying with the CRA requirements are deemed to comply with the AI Act cybersecurity requirements.

4.4. Regulation (EU) 2019/2144 & 168/2013 (Automotive)

Orgalim would recommend clarifying the interaction of the CRA with automotive products regulation, especially Regulations 2019/2144 & 168/2013.

Light vehicles (e.g. 2-wheelers) under EU 168/2013 and (some) automotive spare parts and automotive accessories are covered by the CRA, which might also cover some automotive radio equipment (comparing the RED interaction). There is a risk of unclear or even parallel application (e.g., CRA vs. RED vs. EU 2019/2144) and we therefore recommend that the interaction between the different legislation is clarified.

5. Manufacturers' obligations

5.1. Product requirements of Annex I, especially Annex I.1(2)

As in all NLF legislation, the essential requirements (of Annex I.1) for products are the key to the success of the whole legislation. In the case of the CRA, we note that the level of technical detail of these requirements is already rather high.

Without prejudice to our future contributions, we would like to stress that Annex I.1(2) ("*Products with digital elements shall be delivered without any known exploitable vulnerabilities*") is not precise enough to provide the legal certainty needed. The current language is not in line with the NLF, as "delivered" is not a usual term under the NLF, as opposed to "put into service" or "placed on the market", without going into detail about the respective implications.

Orgalim believes that the current wording of Annex I.1(2) poses a problem, as it operates under the unrealistic assumption that a newly discovered vulnerability could be addressed after production when the product is not under the physical control of the manufacturer, such as in delivery or in storage, and could lead to a hypothetical non-compliance, even if a manufacturer has correctly fulfilled all other requirements of Annex I (1 & 2). It must be possible to remediate vulnerabilities which might become known after a product is placed on the market when it is put into service, e.g. by updating the product, which would concur with the concept of vulnerability management detailed in Annex I.2. This is a common practice and from a security point of view completely sufficient. Additionally, the obligation of the manufacturer should be limited to the making available of, for example, a security update, and he cannot and should not force the user to use it, as there may be sound reasoning, especially in business to business (B2B) environments, to abstain from an immediate update.

Therefore, we strongly believe that the sole existence of a vulnerability discovered after a product is placed on the market but before it is put into service should not constitute a non-compliance of the product, and therefore should not call for a Market Surveillance Authority intervention under Article 43. The CRA must allow for a company to deliver a product with vulnerabilities discovered after being placed on the market when the software had no previously known vulnerabilities. As such, the requirement from Annex I.1(2) must be reformulated in order to avoid the disruption of supply chains.

Additionally, the industry needs to have a clear reference to an EU or a worldwide public vulnerability list/database, recognised by the CRA.

5.2. Reporting obligations (Article 11)

For the sake of proportionality, Orgalim believes that only significantly exploited vulnerabilities should be reported.

This could be done by creating a public list of actively exploited vulnerabilities, like the US Cybersecurity and Infrastructure Security Agency (CISA) catalogue, on which industry components also regularly appear. All vulnerabilities on this list must be agreed internationally and must be looked at by manufacturers (and operators too). CISA already obliges authorities to do so, partly also with time limits.

Moreover, reporting obligations for incidents and vulnerabilities must be aligned with the NIS2 Directive. The strict timeframe for incident reporting (Article 11) where the product manufacturer must notify ENISA about any incident within 24 hours, would probably overwhelm both ENISA and manufacturers regarding quantity and response time. All of this while critical issues might be overlooked in the large number of negligible risks notifications or yield too many false notifications due to insufficient investigations. It would further require disproportionately large investments in technology and dedicated expert personnel, which could weaken the global competitive position of European manufacturers and discriminate against SMEs and others that cannot afford 24/7 product security incident response teams (PSIRTs).

Therefore, we would propose to limit reporting obligations to significant incidents (similar to those required by NIS2) within three working days (similar to those required by GDPR), perhaps combining an "early warning" of significant incidents within 24 hours, and an incident report within 72 hours as required by important NIS2 entities, using already existing PSIRT/CSIRT (product / computer security incident response teams) infrastructures. Moreover, already established international reference points and scoring systems could be referred to, such as the MITRE Corporation reference method for "common vulnerabilities and exposures" (CVE) and the CISA "known exploited vulnerabilities catalogue" (KEV).

Additionally, it would help to clarify how ENISA intends to put the received information to use, taking into consideration the concept of responsible coordinated disclosure.

The envisioned EU vulnerability database of Article 6 of NIS2 will cover a larger scope (NIS entities and its systems) than the CRA, which targets only products (and will not target the cloud vulnerabilities for instance).

Furthermore, Article 11(4) about reporting obligations of manufacturers states:
"*The manufacturer shall inform, without undue delay and after becoming aware, the users of the product with digital elements about the incident and, where necessary, about corrective measures that the user can deploy to mitigate the impact of the incident*."

Due to the supply chain between the manufacturer and the users, the manufacturer does not necessarily have access to (all of) the users and therefore cannot inform them about the incident. Paragraph 11(4) should be rephrased to involve the whole supply chain between the manufacturer and the users.

5.3. Process requirements (Annex I. 1 (2) & (3) (h) + (i), Annex I.2)

Orgalim emphasises the importance of the process-based approach and that requirements addressing the development and design processes *(*for example as they are found in the IEC EN 62443-4-1*)* will be key for the fulfilment of essential requirements currently defined in Annex I.1.

We would like to point out that Annex I.2 sets certain conditions for the manufacturer that might not be appropriate for the industry and B2B settings; in particular the obligation to disseminate patches and make them available free of charge. In the industrial sector, while many patches are made available free of charge, the criticality and complexity of industrial

systems and installations have led us to provide personalised services to clients to push the patching. While patching itself is free of charge, the personalised solution to push and install the patch is commercialised under a contractual agreement.

We encourage the co-legislators to clarify that the dissemination required in Annex I.2(8) is limited to making the patch available and does not include its installation on the product, which is subject to industry process-related specifics (safety) and customer responsibility.

Moreover, Annex I.2(2) requires that vulnerabilities are remediated without delay. However, it requests at the same time a third party certification for security updates for Class I and Class II products. This creates a contradiction between the required speed ("*without delay*") and the length of the required process (third party certification). Orgalim therefore suggests making an exception which allows the manufacturer to proceed with a self-assessment for security updates.

6. Full alignment with the NLF

As Orgalim has expressed on multiple occasions, we fully support the notion that the CRA is a product regulation in line with the NLF, which is a state of the art framework for product regulation in the EU and has a proven track record in ensuring both conformity with legal requirements and the free movement of goods.

Orgalim encourages even further alignment with the New Legislative Framework through the following recommendations.

6.1. Definitions

For the definition of economic operators, we suggest to take over the definitions found in Decision 768/2008 and Regulation 2019/1020.

Regarding terms that are not defined in the framework of the CRA, we suggest creating coherence with other NLF regulations such as, for example, the upcoming Machinery Product Regulation where some of the terms are defined. Other definitions which are currently missing and which should be added as long as there are no already established definitions within NLF Directives and Regulations available to substitute are: "*[significant] incident*", "*sensitive environment*", "*limited attack surface*", "*regular tests*", "*known exploit*", "*cyber*" and "*cybersecurity risk*".

6.2. The role of harmonised standards

Even more important than the coherent use of defined terms is the coherent employment of well-established NLF concepts. One of the most relevant is the role of EN harmonised standards.

In line with the spirit and text of Regulation (EU) 1025/2012, recital 5, harmonised standards "*play a very important role within the internal market*", and "*Technical specifications not adopted by European standardisation organisations do not hold an equivalent status to European standards*" (recital 31 of said Regulation). We therefore suggest to explicitly keep such a key role for harmonised standards also within the CRA. For coherence, it is of the utmost importance to ensure that harmonised standards are the primary and preferred way to detail technical requirements for products throughout the CRA.

Moreover, Orgalim would encourage the development of harmonised standards as 'type-B' standards (generic safety standards, dealing with one safety aspect or one type of safeguard that can be used across a wide range of products),

instead of 'type-C' standards (product standards, dealing with detailed requirements for a particular product or group of products).

Common specifications and CSA Schemes

As an alternative way to define technical details, the CRA mentions common specifications (Article 19 of the CRA) and the cybersecurity certification schemes found in the CSA. However, Orgalim recommends that harmonised standards should always take precedence over common specifications. Indeed, common specifications should only be created in exceptional cases, based on defined criteria. Orgalim strongly recommends defining technical details through the standardisation process, thereby including the industry, and therefore using harmonised standards as the preferred way. In this regard, please refer to an Orgalim position paper that outlines our proposed criteria for common specifications.

Concerning cybersecurity schemes under the CSA, such schemes can only be considered an alternative approach to harmonised standards when their development follows the same principles of transparency and stakeholder participation. Such CSA schemes would have to undergo the same test and assessment procedure as harmonised standards (notably having a verification by a harmonised standards consultant).

However, it is also relevant that for critical products which need a third party certification, the CRA certification does not introduce conflicting requirements with a CSA scheme and vice versa. Only certification that ensures conformity with the essential requirements of the CRA should grant presumption of conformity.

In any case, both the common specifications and the CSA schemes should be a voluntary means to prove conformity with the essential requirements of the CRA.

Interplay with existing standards & certification schemes

The need to build user trust, as well as to establish legal certainty within the market of industrial products with digital elements, are objectives which were identified by the industry a few decades ago. Orgalim wishes to emphasise the long-term continuous investment made by the whole industry in deploying secure development processes and implementing security in the existing portfolio of products based on European recognised standards (CEN CENELEC) such as the EN IEC 62443 and the ISO 2700X series. Under the current wording of the CRA, the long-term industry investment might be penalised in the event that third party certification efforts are doubled.

We would therefore encourage the European Institutions to value existing certification schemes, preserving the competitiveness of the industry through the creation of an equivalency mechanism. This equivalency mechanism should identify a path to apply presumption of conformity to current certification schemes and standards that fulfil the CRA requirements, either by the reference to harmonised standards or in a CSA scheme.

Available IACS certification schemes operated by accredited European Conformity Assessment Bodies (CAB) could also be another path to consider when promoting the harmonisation of certification schemes.

Standardisation request under the RED DA

At this stage, we recall that according to recital 15, Annex I.1 is meant to be aligned with the requirements of the standardisation request M585 for the RED DA Regulation 2022/30. The recital also explicitly refers to the ongoing work in the CEN/CENELEC Working Group 8 of JTC13, working on standards under M585. We hereby underline that considering the findings of that WG will be of the utmost importance for an optimal formulation of the final Annex I.

7. Market surveillance penalties

Orgalim supports the inclusion of the CRA under the Market Surveillance Regulation (EU) 2019/1020 (please refer to our position on market surveillance). As a product regulation, the fines under the Market Surveillance Regulation should also apply for those products with digital elements covered by the CRA. The text of the Regulation should be changed accordingly.

If sales-based penalties are maintained, they should be limited to the respective product sales instead of taking the company's entire sales as a reference to avoid putting companies with a broad product portfolio at a disadvantage.

Furthermore, the CRA should grant the safe harbour from penalties set out in Article 53 to manufacturers of products with third party subcomponents who make efforts in good faith to comply with the CRA. While manufactures may have obligations to recall or patch products, they should not face penalties (set out in Article 53) when they use components from third party suppliers that are later deemed to have vulnerabilities, particularly when manufacturers undertake reasonable due diligence endeavours to comply with the CRA.

Likewise, safe harbours should be given to manufacturers who, despite undertaking reasonable due diligence to ensure accuracy, give market surveillance authorities incorrect information originating from their suppliers (Article 53(5)).

Moreover, we believe that guidance should be issued before any sanctions are implemented.

For more information, please contact: Patrik Fritz, Junior Adviser – Digital, *patrik.fritz@orgalim.eu*

Orgalim aisbl
BluePoint Brussels
Boulevard A Reyers 80
B1030 | Brussels | Belgium

+32 2 206 68 83
secretariat@orgalim.eu
www.orgalim.eu
VAT BE 0414 341 438