Microsoft Policy Position Paper

EU Cyber Resilience Act Proposal

A response to Public Consultation - EU Cyber Resilience Act
January 2023

Executive summary

Microsoft applauds the European Commission's focus on enhancing the cybersecurity of hardware and software, and we are committed to partnering with the Commission and governments globally to reduce cybersecurity risk. We appreciate the opportunity to provide feedback on the September 2022 proposed European Union (EU) Cyber Resilience Act (CRA)[1] and to contribute to the development of this important legislation. The proposed CRA has the potential to not only mandate foundational activities to improve cybersecurity in the EU, but also encourage worldwide adoption throughout product lifecycles, from design to retirement. This approach is consistent with Microsoft's focus and industry leadership on our Security Development Lifecycle,[2] Coordinated Vulnerability Disclosure,[3] and developing and promoting adoption of robust cybersecurity standards and technologies.

This policy position paper outlines our recommendations to the Commission on its proposal and provides our broader perspectives for co-legislators to consider. Microsoft has a long history of advocating for horizontal approaches to information and communications technology (ICT) cybersecurity. Cross-ecosystem consistency and coherence are crucial for the EU's digital single market and can strengthen cybersecurity of interconnected ICT products, services, and components. However, given their complexity, horizontal approaches also involve risks. As Microsoft's submission to the Commission's Call for Evidence on the CRA highlighted in May 2022,[4] a phased implementation can help mitigate these risks. Specifically, we invite the Commission to consider the following recommendations for effective, scalable approaches to driving horizontal cybersecurity improvements:

- Adopt a holistic, phased approach
- Develop targeted measures across the entire ecosystem
- Enable agility and interoperability
- Calibrate and adapt verification methods

Our feedback on the proposed CRA builds on these high-level recommendations, offering ways in which the Commission could further develop, adjust, and refine the CRA proposal to effectively drive security improvements while achieving its envisioned scale. This paper first provides a summary of key recommendations and proposes a more detailed roadmap for the elements of the CRA. Next, it describes and offers recommendations to address foundational challenges that should be prioritised in early phases of a roadmap. Then, it comments sequentially on chapters in the chronological order of the CRA proposal. Finally, two appendices provide additional suggestions targeted at specific language from the proposal and the Annex text to assist experts working on specific sections.

Given the breadth and importance of the CRA, we welcome opportunities to discuss our feedback and to further collaborate on the CRA throughout the policymaking process.

[1] https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act
[2] https://www.microsoft.com/en-us/securityengineering/sdl/
[3] https://aka.ms/cvd
[4] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Cyber-resilience-act-new-cybersecurity-rules-for-digital-products-and-ancillary-services_en

Summary of key recommendations

1) **Develop a more detailed roadmap and public-private partnership process:** The CRA proposal requires products with digital elements meet essential cybersecurity requirements when placed on the market and requires manufacturers to fulfil vulnerability response obligations throughout the product lifecycle. It is appropriately outcome-focused and adaptable. It requires products with digital elements meet essential cybersecurity requirements when placed on the market and requires manufacturers to fulfil vulnerability response obligations throughout the product lifecycle. However, technology and compliance specific details along with key definitions are not part of the proposed regulation. Rather, they can be developed through future collaborative engagements, such as standards development, and established through delegated acts. As a result, the proposal defers many of details about scope and legal compliance for economic operators until standards and conformity assessment criteria are developed or until delegated acts are enacted. This initial lack of adequate or effective guidance, leaves economic operators uncertain about fulfilling their obligations and leaves market surveillance authorities without necessary context to enforce the regulation consistently. Given the complexity of the proposal, a shared understanding of dependencies and sequencing as well as a commitment to stakeholder engagement would raise the confidence of economic operators and other reviewers. A clear roadmap detailing milestones and both the inputs and outputs at each stage (with flexible timelines, as recommended below) would also provide predictability for stakeholders, enabling them to plan and prioritise necessary investments, and a establish a stronger foundation for responsive and constructive feedback.
2) **Plan for capacity building as well as major engineering and operational changes:** Significant capacity building efforts will be required to prepare manufacturers (particularly small and medium-sized manufacturers), other economic operators, conformity assessment bodies, regulators, the European Network and Information and Security Agency (ENISA), and market surveillance authorities and ensure they are well positioned to implement CRA provisions. Many manufacturers will need to increase investments in cybersecurity, cultivate or find cybersecurity expertise, and change practices throughout their product lifecycle. Integrating these investments and changes into the product design, development, and maintenance processes will be time intensive, but will ultimately result in better security and resilience.
3) **Implement the roadmap in phases with flexible timelines:** A detailed roadmap will allow the CRA to adopt an iterative, phased approach to implementation, with each phase resolving ambiguity and simplifying activities for the next phase. A roadmap can also clearly define the success criteria for the completion of each phase. Early phases should specify collaboration mechanisms; resolve ambiguity about scope, definitions, and product categories; define levels of criticality; set expectations for addressing risk at each level; and specify the content of standardisation requests. Later phases should develop open, consensus-based standards used in conformity assessment criteria and should also prepare bodies conducting conformity assessments and the manufacturers seeking the assessments. For example, prior to beginning enforcement, notified bodies could be required to complete a target number of conformity assessments, ensuring both capacity and readiness. In the roadmap's plan for establishing constructive dialogue with key stakeholders, the phases should include mechanisms for economic operators, notified bodies, ENISA, and market surveillance authorities to provide feedback to inform iterative improvements to implementation.
4) **Align with international standards:** Supply chains for ICT products are global and interconnected. In addition, international standards developed by organisations leveraging consensus-based processes reflect industry best practices for cybersecurity. Existing international cybersecurity standards should be used by European Standards Organisations to the greatest extent practical when developing harmonised standards for the CRA. Working to ensure harmonised standards are

aligned with international standards on an ongoing basis will avoid conflicting requirements that disrupt cooperation across regions, thereby: 1.) helping economic operators follow consistent practices in a global market; 2.) enabling consumers to access more products, including those offering best-in-class security; 3.) supporting ongoing security innovation and outcome-focused investments (e.g., ensuring limited cybersecurity expertise is not diverted to redundant activities and instead focuses on new capabilities, products, and components); and 4.) offering an opportunity to simplify conformity assessments so they are less resource intensive and more focused on critical requirements.

Developing the CRA roadmap

ICT manufacturers tackle large, complex product development processes by creating roadmaps and dividing activities into phases. In the planning process, there are an overwhelming number of unresolved issues that, if organised well (i.e., by mapping out dependencies and requirements), can allow work to begin immediately, even as other activities are still being defined and prerequisites are completed. The detailed planning exercise allocates which activities can occur at the same time and establishes phases. Frequently, the product development process transitions from one phase to the next when success criteria are achieved. Managers working on the project can see when critical information will be available, how much time is allotted, and how their deliverables enable subsequent tasks. Ambiguity decreases as the project proceeds because more decisions are made, issues are resolved, and tasks are completed. A project roadmap can also accommodate unanticipated events by being iteratively refined and improved.

The CRA shares similarities to a complex product development process. The overall goals are clear, but, at this early stage, it is challenging for reviewers to understand the roadmap. They will not know when information required for planning will be available, which activities they will need to complete, or how much time they have to complete these tasks. Nonetheless, this information is critical to their continued participation in the EU single market or the very survival of their company.

For manufacturers, it is challenging to determine a viable timeline based on the proposed CRA. Within 24 months of the legislation being finalised and enacted, manufacturers will need to offer products that commenced their planning phase with a risk assessment tied to the essential cybersecurity requirements in Annex I. Manufacturers may now need to wait until harmonised standards are developed and then embark on a long journey to comply. Their work includes conducting a cybersecurity risk assessment, training staff to understand their legal obligations, incorporating new activities into their design and development processes, preparing product conformance materials, enlisting a notified body to conduct a product assessment, creating and publishing an EU declaration of conformity, creating and publishing a vulnerability disclosure policy, creating a security incident response team, working with their suppliers to institute similar processes, and more.

A complimentary set of interdependent and coordinated activities will also need to be performed across other CRA implementation partners, including standards development organisations, market surveillance authorities, ENISA, and the Commission.

A clear roadmap detailing milestones, along with the inputs and outputs of each stage would provide predictability for stakeholders, enabling them to manage ambiguity while planning and prioritising necessary investments. Preparation of the roadmap could identify playbooks for stakeholders with estimated timelines for each activity. Pilot projects, sandboxes, and feedback from economic operators could calibrate the length of activities for different business segments, sizes of enterprises, classes of products, and products with various lead times. For example, due to lead times, CRA requirements for critical products necessitating third party conformity assessments could take more time to enforce than less complex, lower risk products.

Test and success criteria for phases could also be defined and verified. For example, manufacturers may be invited to submit the same conformity assessment materials and product samples to multiple notified bodies to verify consistent results. Metrics could compare the length of time required by notified bodies to complete assessments or quantify the number of assessments they can perform simultaneously to estimate their collective readiness to scale. Market surveillance authorities could be asked to review technical documentation containing conformity assessment materials that had passed or failed conformity assessment by notified bodies to confirm market surveillance authorities have the readiness to reach consistent conclusions.

A phased approach avoids overly prescriptive requirements and makes regulation more sustainable and future proof. In addition, it provides a predictable process as the market adapts to the new rules and allows policymakers to monitor the market impact and improve the framework in each new phase. A critical component for every phase should be open collaboration and stakeholder engagement. Collaborative engagement models provide opportunities to share feedback, provide examples of anticipated challenges, identify best practices, rework approaches with unintended impacts, conduct table-top exercises, add resources or training, and more.

Early roadmap priorities

The section provides recommendations on priorities for the early phases of a roadmap, including foundational issues such as industry engagement. It also highlights areas where greater clarity is required for economic operator preparation and planning.

Continuous collaboration with economic operators

Technical cybersecurity requirements are most effectively defined using iterative processes that are open and inclusive of all stakeholders. Building upon the approach to public consultation in the CRA Call for Evidence and previous legislative efforts (such as the Cybersecurity Act and the Directive on measures for a high common level of cybersecurity across the Union (NIS2)),[5] we encourage the European Commission to establish public-private cooperation mechanisms for the development of technical requirements and other engagement.

In contrast to existing EU cybersecurity legislation, including both Cybersecurity Act[6] and the two NIS Directives, the CRA proposal lacks formal stakeholder involvement. Given the magnitude of the scope of the act and its impact on global economic operators' efforts to improve cyber resilience, Microsoft recommends adding a provision that establishes continuous dialogue between regulators and economic operators. A new industry advisory group or a dedicated working group within the NIS Cooperation Group[7] could provide this function.

Microsoft recommends:

1. Creating a dedicated CRA working group within the NIS Cooperation Group that includes representatives of economic operators.

[5] https://eur-lex.europa.eu/eli/dir/2022/2555/oj
[6] https://eur-lex.europa.eu/eli/reg/2019/881/oj
[7] https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group

Addressing remote data processing solutions

Recital 9 refers to the exclusion of software as a service (SaaS) except for "remote data processing solutions relating to a product with digital elements understood as any data processing at a distance for which the software is designed and developed by the manufacturer of the product concerned or under the responsibility of that manufacturer, and the absence of which would prevent such a product with digital elements from performing one of its functions."

This language results in several challenges for economic operators when determining the remote data processing scope and conformance and creates confusion for regulators focused on enforcement. The first challenge is determining what is covered by product functions. Manufacturers place products on the market as a commercial activity, whether in return for a payment or free of charge. There are many models whereby customers receive a product with digital elements free of charge, but the manufacturer still derives some economic benefit. Examples are the display of advertisements as a user interacts with a product, the collection of data to be sold by the manufacturers to other parties, or opportunities within the product for the user to pay to use enhanced or additional features. Products with digital elements also provide observable features for users, for example, displaying the current temperature based on the measurement from a hardware sensor or displaying the difference between the historical average temperature stored in a remote database and the current temperature. The "functions of a product" could include those that provide economic benefits to manufacturers, observable benefits to users, or some combination thereof.

After determining which functions are relevant, the second challenge is understanding dependencies that might cause a product with digital elements to be unable to perform those functions. In the example of the temperature measuring product above, the display showing the difference between the historical average temperature and the current temperature might depend on the following:

- an internet connection between the display device and the remote database of average temperatures
- the physical hardware the database of historical temperatures resides on
- the database software product used to implement the remote database of historical temperatures

Based on the definition of remote data processing, the situation when a manufacturer only makes the local software and hardware used to measure and display the temperature is simple; none of the bulleted items above are part of the product. However, if the manufacturer is in other lines of business (e.g., providing internet connectivity by operating a subsea cable; providing cloud services that include the physical server used to hold the database of average temperatures; or selling the database product used to implement the database), then those additional items are in scope for remote data processing. As a result, the scope of the product depends on the broader business activities of the manufacturer. In some cases, the scope of the product could depend on where the product is deployed. For example, if a customer deploys the temperature product at a location whose only internet connection to the remote database sends data over the subsea cable the manufacturer operates, then the subsea cable is part of the product.

A third challenge is determining and conducting a conformity assessment when the product scope is variable. The harmonised standards developed for the CRA are unlikely to include conformity assessment criteria the manufacturer would require for subsea cable cybersecurity or operating servers in a data centre. Conformity assessment bodies would need to charge significantly different assessment fees for essentially the same product or be unable to assess them with equal rigor. Moreover, market surveillance authorities will have similar challenges in verifying conformity. In addition to technical product information, they will need to seek information about all the manufacturer's lines of business and determine if any might impact the availability of product functions.

Many of the cybersecurity risks associated with remote data processing can be mitigated by applying the essential cybersecurity requirements at the boundary of the local elements of the product with digital elements (i.e., standalone software, embedded software, and hardware). For example, the requirement to encrypt data in transit impacts the remote data processing solutions that can be leveraged by a compliant product. As another example, consider a solution including a door lock, a smartphone application able to unlock the door, and a service to communicate between them. Whether the service is in scope or not, the essential cybersecurity requirements in Annex I Section 1(3) (b) include the requirement for the door lock to ensure protection from unauthorised access by appropriate control mechanisms.

Given these challenges, the intersecting scope of the CRA with other EU cybersecurity legislation (e.g., the NIS2 Directive as discussed later in this response), and alternative strategies for addressing cybersecurity risks associated with remote data processing, Microsoft recommends removing remote data processing from the CRA scope.

If remote data processing continues to be included in the CRA, the definition of the product scope should clarify whether the hardware used for remote data processing and data transmission are in scope. Remote data processing can be performed in a data centre owned by the manufacturer or on infrastructure leased from a cloud service provider. It would be challenging for manufacturers to provide documentation on hardware if they use a cloud service provider. The definition of the product scope and the conformity assessment for the essential cybersecurity requirements in Annex I Section 1, should be based solely on the product characteristics, not the manufacturer. As a result, the product scope with respect to remote data processing should be consistent and independent from a manufacturer's other lines of business. This will enable conformity assessment criteria to be developed based on product, not manufacturer, characteristics. In addition, the harmonised standards for the CRA should not aim to include platform as a service (PaaS) or infrastructure as a service (IaaS), which are also addressed in other EU cybersecurity legislation. Data processing occurring during the transmission of data between a local product and remote data processing, even if the infrastructure is provided by the same manufacturer, should also be out of scope.

Microsoft recommends:

2. Removing "remote data processing" from the scope of a product with digital elements to avoid confusion and minimise complexity for enforcement (Recital 9 and Article 2), and addressing risks associated with remote data processing by applying relevant essential security requirements at the boundary of the local elements of the product.

Defining risk categories and treatment

Microsoft welcomes the foundational, risk-based approach used in the CRA proposal which is aligned with industry best practices for managing cybersecurity and other risks. For example, the manufacturer's obligations to meet the essential cybersecurity requirements in Annex I Section 1 are based on a risk assessment the manufacturer is required to undertake per Article 10(2). The manufacturer considers the result of the risk assessment during the product lifecycle, complying with the essential security requirements for vulnerability handling in Annex I Section 2. The CRA is also focused on product security features and managing vulnerabilities while a product is on the market; Annex I Section 1(1) says, "Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks."

However, a source of ambiguity is understanding which cybersecurity risks must be addressed. The proposal does not clarify whether manufacturers can leverage threat profiles for different products to inform such risk management activities. The CRA is focused on risks associated with products connected to a device or network (based on Article 2(1)), but cybersecurity is a broad term applied to a range of threats or vulnerabilities, including attacks involving physical access, cybercriminals, nation state threat actors, company insiders, cryptographic weaknesses, supply chain operations, and more. Most cybersecurity risk mitigations are designed to reduce threats designated as "illegal system interference" and unlawful per existing cybercrime legislation.[8] The cost for organisations to fulfil the obligations, particularly vulnerability response and reporting, will correlate to the activity of attackers. Manufacturers will need to rely on conformity assessment criteria to differentiate to regulators whether vulnerabilities or security incidents should be attributed to non-compliance (e.g., a lack of appropriate risk treatment) or the product with digital elements receiving outsized attention by threat actors conducting illegal activities.

This ambiguity is more pronounced with the creation of different risk categories and the recognition that, especially in an interconnected supply chain, all products may be targeted by threat actors. Recital 7 notes all connected products with digital elements provide an opportunity for "malicious actors to gain privileged access to a system or move laterally across systems." Recital 25 then classifies critical products with digital elements, explaining the potential for severe negative impacts to industrial processes, essential entities, the supply chain, and the performance of critical or sensitive functions, such as processing of personal data. Recital 26 further classifies critical products into class I and class II and requires successively stricter conformity assessments. Recital 62 empowers the Commission to adopt acts for highly critical products, including minimum criteria for conformance and supplementary elements for inclusion in technical documentation. With stricter conformity assessments, manufacturers are obliged to perform a more rigorous assessment of cybersecurity risks and a stronger treatment of risks identified. However, the CRA proposal does not set clear expectations for risk treatment across levels of product classification (i.e., default, critical class I or II, and highly critical).

Challenges interpreting these obligations are also exacerbated by the nature of cybersecurity risk. Entities preventing attacks must defend on multiple fronts at all times, whereas malicious attackers may only need to find a single weakness to orchestrate a successful attack. Many cybersecurity attacks rely on social engineering or inadequate installation, configuration, operation, or maintenance of products with digital elements, demonstrating that cybersecurity is a shared activity between economic operators and users. Despite a manufacturer appropriately mitigating risks, a product with digital elements can still be compromised by a supply chain dependency, an insider attack, a compromise of digital infrastructure, or numerous other threats.

Cybersecurity risk is also dynamic in nature. For example, the more a product is deployed, the more valuable it becomes for malicious actors to compromise. In addition, a product that had strong security yesterday can have weak security tomorrow, as new attack tactics, techniques, and procedures (TTPs) are identified by both security researchers and threat actors. Ongoing investments by sophisticated

[8] See Article 3 of the Directive 2013/40/EU of the European Parliament and of the Council of August 12, 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (Link: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013L0040&from=EN)

cyberthreat actors and the sharing of TTPs across the cybercrime economy have resulted in a threat landscape that continues to evolve.

Article 23(2) says, "The technical documentation shall be drawn up before the product with digital elements is placed on the market and shall be continuously updated, where appropriate, during the expected product lifetime or during a period of five years after the placing on the market of a product with digital elements, whichever is shorter." Per Annex V Item 3, the technical documentation includes an assessment of cybersecurity risks against which the product is maintained, and per Annex V Item 4, how assessment criteria was applied to satisfy the essential security requirements in Annex I. Without more clarification, the technical documentation could be a continually moving target for manufacturers to maintain as new attacks emerge and the set of conformity assessment materials (e.g., harmonised standards) increases. It is also unclear if the publication of new conformity assessment criteria retroactively applies to products already placed on the market. In addition to revising the technical documentation of conformity assessment, it is uncertain if the manufacturer is required to modify the product if the prevalent industry practices for treating specific risks change over time.

Microsoft recommends:

3. Defining risk categories (i.e., default, critical class I, critical class II, highly critical) in the CRA along with a process for developing criteria for how the baseline treatment of risk will be assessed for each level. The process should also reflect cybersecurity risks which are constantly evolving and clarify manufacturer's obligations for addressing emergent risks and reacting to potential revisions to conformity assessment criteria (e.g., the publication of a new harmonised standard after a product has been placed on the market).
4. Defining the nature of cybersecurity risks manufacturers are obligated to treat (e.g., attacks involving physical access, supply chain, operational risks, nation state threat actors, etc.).

Options for transferring cybersecurity risk

A common technique for managing cybersecurity risk is to transfer risk and pursue a shared understanding of associated risk management activities. For example, a manufacturer might transfer the risk of a physical attack to users by stating the product needs to be in a physically protected location. Other trade-offs about transferring risk to users may be less clear, though, as cybersecurity frequently challenges manufacturers to balance usability with security. For example, multifactor authentication greatly reduces the likelihood that a user's authentication credentials can be stolen, but it is less convenient for users to provision. Manufacturers could deliver products in a highly secure default configuration that is less convenient to use and then provide warnings and options for users to reconfigure the product to more user friendly, but less secure, configurations. Developing appropriate security defaults as part of the standardisation request for the CRA is a way to address this issue if risk categories and expectations are clarified.

Article 10(4) states, "manufacturers shall exercise due diligence when integrating components sourced from third parties in products with digital elements." However, the definition of "product with digital elements" also includes components which are placed on the market separately. Formalising risk categories could provide a mechanism for the manufacturer to transfer risk to component suppliers when the component is at the same risk categorisation or higher and the manufacturer adheres to user instructions the component provider furnishes. Similarly, remote data processing solutions meeting cybersecurity requirements under the revised NIS2 Directive could provide an additional opportunity for manufacturers to transfer risk.

Microsoft recommends:

5. Explaining manufacturers' ability to transfer risk to users via Annex II "Information and Instructions to the User." Define the level of responsibility the manufacturer retains if the purchaser configures, deploys, or operates a product without appropriate actions to mitigate risk.
6. Identifying the standardisation process for developing guidance for default security settings, which manufacturers should use for different risk categories.
7. Providing a mechanism for manufacturers to transfer risk to component manufacturers (provided the components: i.) comply with the CRA, ii.) address risk at the same or a higher risk category, and iii.) are used in a manner consistent with their instructions to users).
8. Providing a mechanism for manufacturers to transfer risk to services provided by "essential" or "important" entities under NIS2.

Empowering manufacturers to prioritise

The last sentence of Article 10(4), "They [manufacturers] shall ensure that such components do not compromise the security of the product with digital elements should be more risk-based since it requires the manufacturer to unequivocally prevent components from compromising the product with digital elements. This is simply not feasible in practice.

Similarly, the requirements in Annex I Section 1(2) and all of Annex I Section 2 are not treated in a risk-based manner. As written, they will require manufacturers to address every conceivable vulnerability, no matter how minor or inconsequential. Given the threat of potential penalties for non-compliance, this will force manufacturers to divert resources from addressing more significant cybersecurity risks and vulnerabilities toward exhaustively making security updates that provide negligible security benefit.

Microsoft recommends:

9. Framing all essential requirements in Annex I and all manufacturer obligations in Article 10 in a risk-based manner.

Increasing cyber hygiene and the role of users in security

Many cybersecurity incidents result from attackers taking advantage of an individual's or an organisation's poor cyber hygiene. Microsoft estimates basic security hygiene practices protect against 98 percent of attacks.[9] ENISA defines cyber hygiene as "practices that should be implemented and carried out regularly to protect users and businesses online."[10]

Microsoft recommends:

[9] Microsoft Digital Defense Report 2022, p 108 (Link: https://aka.ms/mddr)

[10] ENISA overview of cybersecurity and related terminology (europa.eu) (Link: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology)

10. Complementing the CRA with educational initiatives promoting cyber hygiene for organisations and individuals. Operational cybersecurity risk management requirements, such as those included in NIS2, can also bring focus to cyber hygiene activities.

Developing the standardisation request

The CRA relies on manufacturers conducting cybersecurity risk assessments and treating risk to fulfil the essential cybersecurity requirements in Annex I and other requirements, such as providing information and instructions to the user, per Annex II. The mechanisms used for conformity assessment will guide manufacturers' efforts to achieve better cybersecurity outcomes. The structure in the proposed CRA has the benefit of making the CRA obligations outcome focused, but it also creates significant uncertainty for economic operators.

The conformity assessment procedures for critical products in Article 24 necessitate a firm dependency for manufacturers to fully rely on future harmonised standards, common specifications, and/or European cybersecurity certification schemes. For class II critical products, there is also a reliance on third parties to perform the assessment of the product and manufacturer's implementation of the essential cybersecurity requirements in Annex I. Based on the criteria in Article 6, critical products are essential for security. Without a better definition of critical products - or a full list of these products - it is unclear how requests for harmonised standards can be initiated and completed with ample time to allow notified bodies to perform assessments. Manufacturers will also be challenged to adequately incorporate requirements into the design and development of products. Cybersecurity could be significantly undermined if this approach delays the release of new versions and improvements to critical products, especially security products.

Conformity assessments will be based on yet-to-be-developed harmonised standards, common specifications, and/or European cybersecurity certification schemes. However, the nature of future standardisation requests in conjunction with the CRA is unclear. At a minimum, there could be a standardisation request for a single horizontal standard that provides broad guidance for only covering the essential cybersecurity requirements in Annex I. On the other end of the spectrum, there could be numerous standardisation requests to produce more general guidance for cybersecurity. This may provide details for conducting risk assessments, secure development lifecycle practices, operational security practices, cloud security, network security, human resources management, supply chain risk management, resistance to physical tampering, encryption best practices, organisational risk management, disaster planning, Zero Trust approaches (providing stronger defence in depth), individualised standards for specific classes of products (e.g., toys for children, home routers, etc.), information and instructions for users, technical documentation, practices to mitigate risk from components, etc.

Microsoft recommends:

11. Publishing a draft of the standardisation request to be issued after the CRA is enacted and accepting public comment.
12. Ensuring the standardisation request enumerates the risk categories (e.g., default, critical class I or II, and highly critical) or requests the risk categories to be defined clearly using the standards process.

13. Ensuring the standards developed delineate adequate manufacturer obligations to address threats in each risk category.
14. Ensuring the standards developed include guidance for satisfying the requirements in Annex I and Annex II.
15. Ensuring initial standards are developed for broad categories of products and/or services prior to initiating product specific standards.
16. Requiring the standards developed to identify deviations from requirements in similar existing international standards.

Establishing clear timelines

We commend the Commission's effort to reduce cybersecurity threats quickly. Nevertheless, moving too quickly has the potential to disrupt manufacturers' ability to release new products with digital elements. In addition, the Commission's resilience objectives and the CRA's potential impact could be undermined by rushing security activities rather than taking a more measured and strategic approach.

Article 11 contains reporting obligations for manufacturers. Per Article 57, those obligations start 12 months after the CRA is enacted. Article 11(1) requires manufacturers to report "any actively exploited vulnerability contained in the product with digital elements" and Article 11(2) requires reporting "any incident having impact on the security of the product with digital elements". There is no clarification Article 11 only applies to products with digital elements for which a manufacturer has issued a declaration of conformity, per Article 20. There also is no qualification the reporting requirements only apply for five years after a product has entered the market. Potentially Article 11 places perpetual reporting obligations on manufacturers for any digital product they have ever manufactured.

Article 10(12) says, "From the placing on the market and for the expected product lifetime or for a period of five years after the placing on the market of a product with digital elements, whichever is shorter, manufacturers who know or have reason to believe that the product with digital elements or the processes put in place by the manufacturer are not in conformity with the essential cybersecurity requirements set out in Annex I shall immediately take the corrective measures necessary to bring that product with digital elements or the manufacturer's processes into conformity, to withdraw or to recall the product, as appropriate." However, the CRA proposal does not include a definition for "expected product lifetime.". It is not clear if the manufacturer or some other criteria determines the "expected product lifetime." This makes the timeline for obligations for manufacturers ambiguous.

Article 57 says all the articles apply 24 months after the CRA entry into force. Many products with digital elements take longer than 24 months to design, develop, and deploy. In Article 10(2), the CRA requires manufacturers consider the outcome of an assessment of the cybersecurity risks associated with the product with digital elements "during the planning, design, development, production, delivery and maintenance phases." Realistically, manufacturers are unable to initiate planning or design of a product with digital elements intended to be compliant with the CRA obligations until conformity assessment information has been provided through harmonised standards, common specifications, or European cybersecurity certification schemes.

Finally, the text does not provide clear timelines for manufacturers to comply with the requirements when they are updated (Articles 10(15) and 23(5) provide examples). We believe setting a clear timeline for compliance with updated rules and frameworks, as established in the delegated and implementing acts, would improve clarity for manufacturers.

Microsoft recommends:

17. Specifying a maximum duration for reporting obligations in Article 11 and specifying those reporting obligations only apply to products with digital elements for which the manufacturer has drawn up an EU declaration of conformity, per Article 20.
18. Defining the term "expected product lifetime" as the lifetime a manufacturer documents in the information and instructions to the user, in Annex II Item 8 (i.e., "until when users can expect to receive security updates").
19. Providing adequate time for manufacturers to plan and design new products after conformity assessment criteria is available or when products are categorised with a higher criticality (e.g., a category of critical products is added or modified in Annex III).
20. Using a risk-based approach to define criteria for specific timelines in place of the terms "continuously updated" (used in Articles 20(2) and Article 23(2)) and "regular" (used in Annex I Section 2(3)), "without delay" (used in Annex I Section 2(2) and Annex I Section 2(8)), "timely manner" (used in Annex I Section 2(7)), "without delay" and "without undue delay" (the latter two are used extensively in articles).
21. Providing specific scoping and timelines for compliance with implementing and delegated act regulations adopted by the European Commission in relation to the CRA.

General provisions (Chapter 1)

Leveraging a phased approach

As horizontal cybersecurity legislation, the proposed CRA covers a broad range of products entering the EU market. We encourage co-legislators to consider how the wide scope and ambiguous elements may create confusion among regulators and economic operators, ultimately impacting the availability and cyber resilience of products in the digital single market.

Hardware, software, and services are distinct categories with integrated development processes and shared dependencies. For example, a hardware device manufacturer has strong control over its own incremental contributions to a final product, building upon elements sourced from suppliers and the broader ICT ecosystem. However, the manufacturer must continuously adapt the product to support it throughout its lifecycle, based on the way its ecosystem elements evolve (or stop being produced or supported). These elements often include software and network-connected services which may be impacted by security practice and conformity assessment expectations associated with connected devices.

As manufacturers are sourcing components and services when the CRA initially comes into force, they will likely be challenged to find components that adequately comply with CRA requirements. Ideally, the availability of components and services adequately addressing cybersecurity risks will increase over time due to the CRA.

In addition, manufacturers of products with digital elements do not recreate the hardware, software, and services from scratch for each new product. Most often, a new version of a product utilizes the same software code as the previous version with minor improvements and the addition of more features. The development of a new version of a product rarely involves a major refactoring of its entire software code base and complete software rewrites can introduce new problems.

When manufacturers adjust their practices to comply with the proposed CRA requirements, they will be challenged to address all cyber risks in a single release. Initially manufacturers are likely to heavily rely on their vulnerability response processes to maintain security during the product lifecycle. This is because their product planning, design, and development activities will only change a small amount of their product code with each release. As manufacturers adopt more security aware practices and successively refactor larger amounts of their products using the practices, their reliance on vulnerability response will decline as their products experience fewer security vulnerabilities.

The CRA can become a global "lighthouse" regulation by proposing innovative requirements in a new structure, requiring enforcement across the EU, and implementation by the wider industry. Microsoft recognises the potential of this legislation and strongly advises a gradual, well-defined approach and corresponding detailed roadmap for its successful application. Regulators and market surveillance authorities should consider the challenges economic operators will face sourcing more resilient components and services and incrementally refactoring their software code after adopting more security aware practices.

Microsoft recommends:

22. Implementing the CRA in phases, expanding the scope of impacted technologies and/or emphasis on required practices over time. For instance, compliance obligations could initially focus on manufacturers implementing more secure development practices, improving their ability to respond to vulnerability reports, generating security updates, and helping users deploy patches rather than addressing risks across their entire software code base immediately.

Intended scope of distributors

When applying the New Legislative Framework (NLF) to software products and components there is a need for greater clarity regarding the intended scope of "distributor" and consistency with existing legislation. It is unclear whether code hosting and collaboration platforms or package repositories would be interpreted as distributors or hosts of content.

Notably, the Digital Services Act (DSA)[11] provides conditional exemption of liability for hosting content, as does the Copyright Directive[12] for open source software development and sharing platforms. The Commission's Product Liability Directive (PLD) proposal[13] acknowledges the DSA exemption for online platforms, with this guidance about applying the exemption under the PLD recital 28, "When online platforms perform the role of manufacturer, importer or distributor in respect of a defective product, they should be liable on the same terms as such economic operators[…] In keeping with this principle, when online platforms do so present the product or otherwise enable the specific transaction, it should be possible to hold them liable, in the same way as distributors under this Directive. That means that they would be liable only when they do so present the product or otherwise enable the specific transaction, and only where the online platform fails to promptly identify a relevant economic operator based in the Union".

Code hosting and collaboration platforms, including GitHub and servers hosted by individuals and organisations, support the development of software components by enabling interested developers to

[11] https://eur-lex.europa.eu/eli/reg/2022/2065/oj
[12] https://eur-lex.europa.eu/eli/dir/2019/790/oj
[13] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12979-Product-Liability-Directive-Adapting-liability-rules-to-the-digital-age-circular-economy-and-global-value-chains_en

obtain and contribute to source code and precompiled binaries. Package repositories, including npm[14] and NuGet[15], support the development of software products by enabling developers to locate and download components they can use to develop products. Unlike app stores, which curate and review published apps (i.e., end products) and facilitate transactions between manufacturers and consumers, package repositories along with code hosting and collaboration platforms provide a content platform enabling access to components using both open source and proprietary licenses.

Microsoft recommends:

23. Excluding software package repositories as well as code hosting and collaboration platforms from the definition of distributor given the role they serve in facilitating innovation and research and the manner they host content (Article 3(21)).

Aligning free and open source software treatment with industry practices

Microsoft supports the CRA proposal's exemption for free and open source software (as articulated in Recital 10), given the globally distributed and community-centric nature of open source projects. Regulating free and open source software (OSS) would hamper innovation and research[16] and involve significant implementation challenges.

Explicitly stating an OSS exemption in Article 2(5) and defining the scope and impact of "commercial activity" as it pertains to open source would improve clarity for the open source community. There is ambiguity resulting from the intersection of OSS with "commercial activity," both in the context of infrastructure and services provided to open source projects and with regard to activities that open source projects may pursue while building OSS.

Consistent with our recommendation regarding package repositories and code hosting and collaboration platforms, the infrastructure and services provided to open source projects should be out of scope, regardless of commercial status. Hosting of source code control systems, build infrastructure, security scanning, and package registries is often provided by commercial and non-profit entities to open source projects at no cost (though these entities may derive commercial benefits, such as through advertising, to offset the costs of providing services). Disincentivising entities to provide infrastructure and services at no cost would dramatically reduce the options for open source projects, depriving the open source community of critical resources enabling them to more securely develop and deliver software.

Commercial services enabling the effective use of OSS, such as technical support and consulting services, should also be out of scope and not bring OSS offerings into scope. Many consumers of open source software depend on third parties to provide deployment, configuration, and operational services. These services, often provided by small and medium-sized enterprises, range dramatically in their focus and complexity, from creating themes for the software to match the consumer's brand, to integrating the OSS with the consumer's other software, to installing, updating, and configuring OSS products for the consumer. Providers usually do not have influence over the open source project and are unable to

[14] https://www.npmjs.com/about
[15] https://www.nuget.org/
[16] https://digital-strategy.ec.europa.eu/en/library/study-about-impact-open-source-software-and-hardware-technological-independence-competitiveness-and

assume any obligations that could otherwise fall to a distributor or importer of a commercial product (unless a provider has substantially modified the open source software or is packaging it as part of a commercial product).

Open source projects may also receive financial support in various ways. For example, private sector employees may work on specific open source projects, open source projects may receive sponsorships from individuals or companies, and open source developers may provide paid consulting services related to the open source project. These types of financial support should not be deemed commercial activity unless the open source software is packaged as part of a commercial product.

Microsoft recommends:

24. Explicitly adding an exemption for OSS in Article 2(5) such as, "This Regulation does not apply to free and open-source software, including its source code and modified versions, except when such software is provided as a paid or monetised product."
25. Excluding providers of services to open source projects from importer and distributor obligations, even if they derive indirect commercial benefit from the provision of these services.
26. Excluding technical services for open source software from manufacturer, importer, and distributor obligations unless the provider of the service is providing the customer a substantively modified version of the open source software.
27. Ensuring financial support for open source projects is not deemed "commercial activity" and does not necessarily bring the open source software produced by that project into the scope of the CRA.
28. Clarifying the intent of the above recommendations with a revised Recital 10 as described in Appendix I of this response.

Defining critical products and categories

The CRA proposal suggests four levels of product categories: default, critical class I, critical class II, and highly critical. The CRA's definition of critical products and its enumerated list of critical product categories (i.e., class I and II) in Annex III are designed to be adjusted over time. Criteria for the determining which products are class I versus class II is needed along with an explanation of why some product categories are not listed at all. Adding a provision requiring active, regular, and structured stakeholder consultation regarding any modification of the definition, scope, or enumerated list of critical product categories in Annex III – as well any modification of the list of highly critical products with digital elements – would address ambiguity and future proof the Commission's approach. Clarity regarding the intent of Annex III would support manufacturer planning and confidence in readiness. For example, articulating whether the goal is to develop conformity assessment criteria (e.g., harmonised standards) specialised for each critical product category or for manufacturers and notified bodies to adjust the treatment of risk by those products.

Microsoft recommends:

29. Populating and updating the critical product definitions (Article 6) and categories (i.e., Annex III) using a clear, risk-based approach supported by a transparent and inclusive methodology so economic operators and regulators can understand the rationale and accurately classify products.
30. Regarding Article 6 and Recital 27, clarifying in Article 6(3) and 6(5) that invoking the adjustment of Annex III by the European Commission can only follow an extensive public consultation, either under the EU Better Regulation or through a platform where economic operators in scope of the CRA are able to consult the European Commission, National Competent Authorities (market surveillance authorities), and ENISA on the impact or necessity of adjusting the list. Moreover, clarify how and when products can be excluded from Annex III or moved from highly critical to default level, and vice versa.
31. Adding the following to Article 6: "When exercising the power of delegation outlined in point 2, 3, and 5 of the Article, the Commission shall conduct thorough public consultations and engage in regular and structured dialogue with industry stakeholders to gather evidence and evaluate market implications of including or withdrawing categories of products in scope."

Fostering regulatory consistency

Given the complexity of CRA provisions related to enforcement, Microsoft recommends institutional cooperation among the European Commission's Directorate-General Departments responsible for developing and implementing related cybersecurity policies. The cooperation should be a structural mechanism that is transparent and inclusive to minimise siloed policy development, encourage coordination, and foster inclusion of cybersecurity expertise with other policy domains, such as sustainability.

Microsoft welcomes the European Commission's consideration for existing legislation (Regulation 2017/745, Regulation 2017/746, Regulation 2019/2144) to avoid regulatory overlap of security requirements and unintended duplicative reporting obligations. However, we share the wider industry concern about potential overlap between the requirements defined in the NIS2 Directive and the CRA, since both regulations impact cloud services. We believe reporting requirements in the CRA should be harmonised with NIS2. Below, we outline our approach for enabling interplay between the CRA proposal and key legislation including the NIS2, the Delegated Regulation (EU) 2022/30[17], and the AI Act.

Eliminating reporting obligation conflicts with the NIS2 Directive

The proposed CRA complements the recently adopted NIS2 Directive. The CRA seeks to enhance cybersecurity during the design, development, distribution, and maintenance of digital products while NIS2 focuses on operational cybersecurity in organisations that qualify as "essential" or "important" entities.

However, there is considerable overlap between the proposed CRA and NIS2, as many organisations covered by the NIS2 Directive – including cloud computing service providers, electronic communication service providers, and computer and electronics manufacturers – may also be regulated under the CRA as manufacturers. CRA co-legislators should be mindful of this overlap between NIS2 and the proposed CRA and strive to eliminate conflicts and redundancies between the two legislations.

[17] https://eur-lex.europa.eu/eli/reg_del/2022/30/oj

Mandatory incident reporting is one of the primary ways both the proposed CRA and NIS2 will regulate covered entities. Microsoft strongly supports the creation of consistent reporting obligations to enhance cybersecurity. However, the proposed CRA would create conflicting incident reporting obligations for some organisations in certain circumstances. Fortunately, these conflicts can be easily resolved. Under Article 23(1) of NIS2, a covered entity must report the occurrence of "any incident that has a significant impact on the provision of their services" to a relevant government agency, either a national computer security incident response team (CSIRT) or national competent authority (NCA). Incident notification under this article follows a 24/72 hour reporting period which means a regulated entity must provide early warning of incidents to the agency within 24 hours of becoming aware and must submit a notice with additional information within 72 hours.

NIS2 streamlines incident reporting by a covered entity and ensures broader governmental situational awareness by mandating interagency information sharing, including sharing information across EU Member States. When the agency receiving an incident notification determines it is justified or when an incident concerns two or more EU Member States, the receiving agency must inform other EU Member States and ENISA of the incident and share the information provided by the notifying entity. The streamlined reporting channel for entities responding to an incident minimises the impact on resources needed for incident response.

The current CRA proposal conflicts with this NIS2 Directive framework and will complicate incident reporting in certain situations. Under Article 11(1) of the proposed CRA, a manufacturer must report to ENISA any active exploit of a vulnerability, along with additional information, within 24 hours of becoming aware of the exploit. This same 24 hour reporting obligation applies to "any incident having impact on the security of the product." There may be occasions when such an exploit constitutes a significant incident that must be reported under NIS2 (and national legislation transposing NIS2). In such a situation, the proposed CRA would impose a conflicting and competing reporting obligation on the covered entity because the CRA does not employ the 24/72 hour early warning/notification reporting framework established in NIS2, and it requires reports to ENISA in addition to notices to a CSIRT or NCA under NIS2. Thus, the CRA reporting requirement risks detracting from the focused reporting process under NIS2.

To resolve this problem, co-legislators should revise the proposed CRA to include an exception to the reporting obligation for matters that qualify as incidents subject to reporting under NIS2. This exception should explain that when a vulnerability exploit under Article 11(1) or an incident under Article 11(2) is subject to notification requirements under Article 23 of NIS2, then notification under Article 23 of NIS2 will satisfy any reporting obligation under the CRA. ENISA, computer security incident response teams (CSIRTs), and competent authorities are well positioned to establish and manage communication and information-sharing procedures among themselves. Care should be taken to avoid redundancies and unnecessary burdens on entities covered under both the CRA and NIS2, especially when organisations are responding to a cybersecurity incident.

In addition, the proposed CRA should be revised to conform to the 72 hour reporting period used in NIS2. A 72 hour reporting period will allow adequate time for manufacturers to investigate, gather information, and respond to exploits and incidents while providing timely notice to ENISA. This period is better aligned with security objectives and internationally recognised best practices (e.g., in the General Data Protection Regulation (GDPR)[18] and the German IT Security Act 2.0).[19] NIS2 employs a 24 hour early warning for certain incidents where there is a need for earlier situational awareness and

[18] Regulation (EU) 2016/679 of the European Parliament (Link: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679)

[19] https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl121s1122.pdf

requires only limited notice. The proposed 24 hour reporting in the CRA does not rest on similar exigencies. Establishing consistent reporting periods will promote efficiency and focus on incident response activities by allowing organisations to integrate CRA and NIS2 reporting into the same business operations.

Microsoft recommends:

32. Appending to Article 11(2):

    > "economic operators that are also identified as essential entities or important entities under the Directive [NIS2] and who submit their incident notification pursuant to the Directive [NIS2] should be deemed compliant with Article 11(2) of this Regulation."

33. Revising Article 11(1) – "…in any event within 72 hours of becoming aware…"
34. Revising Article 11(2) – "…in any event within 72 hours of becoming aware…"

Harmonising with the Radio Equipment Directive

We welcome Recital 15, which recognises an overlap between the CRA proposal and the Delegated Regulation (EU) 2022/30 as well as the related standardisation request. However, we request clarifying the language to indicate clear legislative precedence of the CRA over the requirements in the Delegated Regulation (EU) 2022/30 to improve the harmonisation of the cybersecurity regulatory framework and clarify compliance processes.

Microsoft recommends:

35. Clarifying the repeal or amendment intent with regards to Delegated Regulation (EU) 2022/30 by articulating a clear legal solution.
36. Clarifying the relationship between the Delegated Regulation (EU) 2022/30 and the CRA when both are applicable by adding an amendment in the core of the legal text of the CRA stating that compliance with the CRA means a presumption of conformity with Article 3(3) (d), (e) and (f) of Delegated Regulation (EU) 2022/30.
37. Clearly affirming the standardisation work in the Delegated Regulation (EU) 2022/30 standardisation request shall be considered in the preparation and development process of harmonised standards for the CRA.

Aligning with the AI Act

In addition, we welcome the effort to align the conformity assessment procedures under the CRA and the AI Act for products with digital elements classified as high-risk AI systems under the AI Act. However, further clarification is also required in this area.

Microsoft recommends:

38. Revising Article 8(3) to indicate whether manufacturers of high-risk AI systems listed in CRA Annex III require two conformity assessments under both regulations. Microsoft recommends the same procedure as described in Article 8(2) to avoid burdening entities and conformity

assessment bodies. By aligning assessment processes, the legislator will improve efficiency of the notified bodies and will benefit the conformity work within the CRA.

39. Clarifying the enforcement framework between the CRA and the AI Act in Article 41(10) and the role of market surveillance authorities in the context of high-risk AI systems. We specifically recommend identifying the market surveillance authorities receiving information about an incident or vulnerability notification or – if both the CRA and the AI Act market surveillance authorities will be informed – in the order information is shared by ENISA.

Obligations of economic operators (Chapter 2)

Essential requirements (Annex I Section 1)

Addressing component resilience and assessment in isolation

Some product-oriented essential security requirements - as well as labelling, documentation, and conformity assessment requirements - may be ill-suited for components not intended as end user products. For example, a manufacturer selling user interface design components, which are non-functional until used to build a product, will rely heavily on the "where applicable" phrase in Annex I Section 1(3) to attest to the component conformance. As a result, it creates challenges for manufacturers to apply requirements to components and for assessors to determine their conformance with requirements.

The component requirements will vary and very few - or even none - of the requirements in Annex I Section 1(3) may apply to some components. In such cases, applying the CE mark to components not intended as an end user product may undermine the value of the CE mark in signalling whether the product satisfies the essential cybersecurity requirements in Annex I.

In addition, if a component not intended as an end user product belongs to a category requiring standardisation or assessment, then it is critical the standards development and assessment processes specifically consider the differences between components and end user products. For example, a standard may make some requirements optional for components, and an assessment process may account for some components or aspects not functioning when not incorporated into an end user product.

Microsoft recommends:

40. Holding further consultations with manufacturers, standards bodies, and assessors to determine appropriate approaches to requirements and assessments for components not intended as finished, end user products.

Protecting sensitive technical documentation and translation

In general, Microsoft supports the use of technical documentation. However, Article 10(3), as written, is concerning because it lacks mechanisms to protect information contained in a risk assessment and associated documentation set forth in Article 23 and Annex V. Sensitive security information and intellectual property (including confidential trade secrets, that could increase security risks or place a business at a competitive disadvantage if they were mishandled) are likely to be included. For example, the sensitive information required could extend to vulnerability-related data or schema that facilitates the discovery and exploitation of a vulnerability. To mitigate these risks, we urge the development and application of safeguards and security standards for any person accessing or otherwise utilising such information in carrying out a function under the CRA. Regarding "translation" of technical documentation, Microsoft recommends using English as the "language understandable by the market surveillance authorities" to avoid administrative burden and misinterpretation during translation.

Microsoft recommends:

41. Requiring the development and use of appropriate safeguards to protect sensitive data included in technical documentation.
42. Adding "… English or other language easily understood …" to Article 10(13).
43. Requiring "Technical documentation shall be drawn for the market surveillance authorities exclusively for the purposes of their supervision activities and cannot be shared further or disclosed by the market surveillance authorities."

Promoting greater exchange and benefits of software bills of materials

Products with digital elements will be composed of hardware and software components from multiple manufacturers, some of which will originate from outside the single market. Software bills of materials (SBOMs) are most accurate when produced during the development of individual components and then combined to produce SBOMs for final products. This requires interoperability between SBOM formats used by products manufactured in the EU and those manufactured elsewhere, making adoption of international SBOM standards and conventions important.

Microsoft adopted the Linux Foundation's SPDX standard[20] (ISO/IEC 5962),[21] identified by the US National Institute of Standards and Technology (NIST) as one of three SBOM standards meeting the requirements of the US Executive Order 14028: Improving the Nation's Cybersecurity[22] (others are CycloneDX[23] and SWID Tags).[24] We encourage cooperation between the EU and the US on international SBOM standards through participation in international standards bodies and community engagements, such as the SBOM Workstreams[25] convened by the US Cybersecurity and Infrastructure Security Agency (CISA).

Microsoft has been investing in technologies for storing and exchanging supply chain security compliance artifacts and attestations, such as SBOMs. These technologies would allow SBOMs to be independently verified and would enable automated and continuous assurance based on attestations. Supply Chain Integrity, Transparency and Trust (SCITT)[26] offers one approach for storing and exchanging supply chain artifacts and attestations, enabling users to verify conformance with their supply chain security requirements.

Microsoft intends to use technologies, including SCITT, in combination with open international standards, to continuously exchange trusted supply chain information, including information from the open source community. This continuous exchange of trusted supply chain information helps verify the

[20] https://devblogs.microsoft.com/engineering-at-microsoft/generating-software-bills-of-materials-sboms-with-spdx-at-microsoft/
[21] https://www.iso.org/standard/81870.html
[22] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
[23] https://cyclonedx.org/
[24] https://csrc.nist.gov/Projects/Software-Identification-SWID
[25] https://www.cisa.gov/sbom#CISA-SBOM-Workstreams
[26] https://scitt.io/

integrity of supply chains, share threat intelligence information, and detect supply chain attacks in an automated, scalable way. We encourage coordination and collaboration from European Institutions, EU Member States, and other partners on SCITT and related efforts to build technologies responsive to government interests and concerns.

When considering SBOM requirements in the context of CRA, it is important to realise that SBOMs, are still evolving, particularly those at the scale of CRAs proposed scope. It will take time for SBOM requirements to flow to upstream suppliers (which may be several levels deep) and for updated products containing SBOMs to flow back to their consumers. During this time, SBOMs may have reduced accuracy and be less complete as participants in the supply chain may need to use software composition analysis (SCA) tools to synthesize missing SBOMs.

Microsoft recommends:

44. Incentivising increased transparency in supply chains and recognising the evolving nature of SBOMs by limiting potential liability and penalties that may arise from this transparency (e.g., if, in early stages, there are inaccuracies in SBOMs that provide information beyond top-level dependencies).
45. Evaluating incentives and investments to accelerate SBOM adoption and the exchange of trusted supply chain information among economic operators.
46. Collaborating in the development of international SBOM and other supply chain cybersecurity standards to ensure they address the needs of the EU single market.

Reporting obligations

Vulnerability reporting

Effective and responsible cybersecurity requires cooperation throughout the entire security ecosystem and Coordinated Vulnerability Disclosure (CVD) is a vital mechanism for sharing information about and mitigating security vulnerabilities. No product can be fully secure or absent of vulnerabilities and security researchers play an integral role in the ecosystem by discovering vulnerabilities missed in the software development process and providing the information to entities able to action it to improve their own products and overall ecosystem security.

Under the principle of CVD, researchers disclose newly discovered vulnerabilities in hardware, software, and services directly to the affected product's manufacturer; to a national CERT or other coordinator who will report to the manufacturer privately; or to a private service that will report to the manufacturer privately.[27] The researcher provides the manufacturer an opportunity to diagnose and offer tested updates, workarounds, or other corrective measures before any party publicly discloses detailed vulnerability or exploit information. The manufacturer coordinates with the researcher throughout the vulnerability investigation and provides the researcher with updates on case progress. Upon release of an update, the manufacturer may recognise the finder for the research and privately report the issue. If attacks are underway in the wild and the manufacturer is still working on the update, then both the researcher and manufacturer collaborate to provide early public vulnerability disclosure to protect

[27] A security researcher should not be required to exclusively report a vulnerability to any single entity for further coordination. Using the government exclusively for coordination runs the risk of prolonging the time it takes to develop and distribute a patch and may also disincentivise researchers who may want to be recognised and rewarded for their work. Government-led coordination of vulnerability disclosures also sets a precedent for other governments that may stockpile reported vulnerabilities for cyber-offensive purposes rather than reporting them to the manufacturer.

customers. The aim is to offer timely and consistent guidance for customers to address vulnerabilities while minimising the likelihood of revealing vulnerability information to attackers before patches are available to customers.

Encouraging companies to implement a model CVD policy set forth by the EU and ENISA and aligned with best practices would improve the security posture of the EU and foster better security practices among economic operators. (Note : Microsoft's internal approach[28] to vulnerability disclosure aligns with ISO/IEC 29147.[29] In addition, the Software Engineering Institute at Carnegie Mellon University published the CERT Guide to Coordinated Vulnerability Disclosure.[30]) However, the Commission should recognise the CRA's broad scope means the level of CVD readiness across economic operators will vary greatly. Prematurely requiring CVD policies and processes without sufficient education for economic operators may undermine the communication and cooperation necessary to achieve a positive security outcome. Our experience and information in public surveys[31] demonstrate the importance of readiness for effective communication with security researchers and between affected manufacturers. Economic operators should receive sufficient context in vulnerability reports or a mechanism to facilitate coordination. They should also be staffed with adequate resources (or outsource efforts) to address reports in a timely manner. Given these challenges, the Commission should initially work with ENISA to establish a model CVD policy, then engage in a deliberate campaign to encourage and track the implementation of CVD policies by economic operators placing products with digital elements on the market.

Microsoft recommends:

47. Establishing a model CVD policy and then engaging in a deliberate campaign to encourage and track the implementation of CVD policies by economic operators.
48. Encouraging researchers to leverage CVD processes by disclosing newly discovered vulnerabilities in hardware, software, and services directly to the manufacturers of the affected product; to a national CERT, CSIRT, or other coordinator – or to a private service - that will report to the manufacturer privately.

Vulnerability databases

Given the TTPs of advanced cyberthreat actors, we caution the EU against a centralised registry of unpatched or unmitigated vulnerabilities. A centralised repository of unresolved vulnerabilities would become a high value target, especially for nation state actors that stockpile zero-day vulnerabilities to use as cyber weapons.

If the European vulnerability registry contemplated in NIS2 Article 12(2) is intended to only maintain information about vulnerabilities with patches or other mitigations available, then we encourage the Commission to consider the added value of a separate registry against the confusion that may result from disparate registries containing disparate or conflicting vulnerability information. Building infrastructure and submission and management processes for such a registry not only requires major resources and time, but also adds complexity and cost to vulnerability reporting and querying. At a

[28] https://www.microsoft.com/en-us/msrc/cvd
[29] https://www.iso.org/standard/72311.html
[30] https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf
[31] https://ntia.gov/blog/improving-cybersecurity-through-enhanced-vulnerability-disclosure

minimum, we recommend EU collaboration with the CVE® Program[32] to strengthen consistency, minimise duplication, and ensure it can meet the needs of and be responsive to the EU single market.

Microsoft recommends:

49. Revising Article 11(1) to only require reporting of patched vulnerabilities to ENISA, but within 72 hours after the patch is available. (Note: This explicitly removes any requirement to report actively exploited vulnerabilities contained within a product with digital elements.)
50. Adding a citation in Article 11 to ISO/IEC 29147 and using it as the baseline for reporting vulnerabilities as part of a wider EU CVD framework promoted by ENISA.

Public recognition and bug bounties

Public recognition and bug bounties motivate security researchers to discover and report security vulnerabilities. Microsoft significantly invests in bug bounty programs to guide efforts to continuously improve the security of our products.[33] Other economic operators prepared to respond to and investigate a high number of researcher reports should invest in similar policies, as our experience demonstrates that close partnerships with researchers makes customers more secure. All economic operators with a CVD program should also consider the value of and pursue processes to support public recognition for security researchers. Even if a discovered vulnerability is not covered under an existing bounty program, Microsoft publicly acknowledges contributions after we fix the vulnerability and all vulnerability submissions are counted in our Researcher Recognition Program[34].

Microsoft recommends:

51. Encouraging economic operators responsible for placing products with digital elements on the market to establish public recognition and, as appropriate, bug bounty programs.

Conformity of the product with digital elements (Chapter 3)

Conformance verification is the final element to enhance the cyber resilience of products with digital elements. Microsoft supports defining effective, practical approaches to ensure in scope products conform with cybersecurity practices. This requires an understanding of the benefits and drawbacks of existing methods as well as investment in new methods offering greater scale and impact. The calibration of the CRA’s conformance verification methods should be based on needs and challenges today as well as the future to maximise cybersecurity benefits while managing market impact.

Today, costs and infrastructure challenges impact readiness and effectiveness of certain methods of conformity assessment, including third-party certifications. Risk management goals and costs must be balanced to apply appropriate methods in different circumstances. Investments in both workforce

[32] https://www.cve.org/

[33] https://www.microsoft.com/en-us/msrc/bounty

[34] https://www.microsoft.com/en-us/msrc/researcher-recognition-program

initiatives and innovative technology solutions, such as SCITT, could enhance conformance verification options and cybersecurity transparency.

Adopting a phased approach

While a holistic approach that enhances the cyber resilience of products with digital elements used across the ecosystem is ultimately and appropriately the goal reflected in the CRA proposal, phasing implementation allows iterative policy efforts to be improved upon and expanded over time, ultimately supporting more rigorous implementation. Many governments are taking a phased approach to implementing cybersecurity policies. For example, the EU has phased in the development of cybersecurity certifications resulting from the Cybersecurity Act,[35] allowing for iterative learning and process improvements throughout the process. In the US, given the breadth of software in scope for Executive Order 14028, NIST proposed[36] a phased approach to defining "executive order critical software" for which US agencies need to apply elevated, user-focused security measures.[37] NIST also proposed focusing first on standalone, on-premises software in which agencies are solely responsive for operational risk management, but also recognised all forms of software, including software embedded in devices or hardware components and cloud services, should ultimately be in scope.

Various methods could be applied for phasing the cybersecurity requirements and conformity assessments within the CRA framework. In general, by first establishing basic core tenets of security practices and implementing them across a broad swath of products and services, governments can create a regulatory foundation that accommodates industry-wide standards while also preparing for layered tiers of elevated standards to be phased in over time. They can prioritise security practices widely applicable across use scenarios and products with digital elements, such as secure software development practices, patching, and implementation of multifactor authentication. They can also survey impacts, address concerns, predict future advancements and risks, and effectively tailor solutions using the evidence and foresight provided by early phases. As such, a phased approach to CRA implementation based on the category of products could start from less critical products and move to more critical products. Horizontal harmonised standards for default categories of products are likely to be developed more quickly than more complex standards specialised for critical product categories that seek to treat risk more rigorously. Also, design, development, and production of many critical product categories listed in Annex III require significant lead time compared to those included in the default product category.

Microsoft recommends:

52. Using a phased approach for CRA implementation by adopting mandatory requirements for default categories of products based on self-assessment, then gradually moving to more critical categories requiring third-party attestation and certification. This will allow:

    1) economic operators to monitor and evaluate implementation through phases to calibrate the requirements and conformity procedures based on the observed market impact; and
    2) the preparation of notified bodies as well as the development of standards and certifications for the latter stages while the first phases of implementation are ongoing, thus using time and resources more efficiently.

[35] https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act
[36] https://www.nist.gov/system/files/documents/2021/10/13/EO%20Critical%20FINAL.pdf
[37] https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/security-measures-eo-critical-software-use

Developing conformity criteria

The presumption of conformity to a regulation can be best ensured if a product with digital elements is designed to comply with harmonised standards. This allows general regulatory requirements to be defined in more technical detail within standards. Adapting and including the requirements mentioned in harmonised standards would have the additional benefit of reducing the cost and burden of compliance. Compliance can be a resource intensive activity within an organisation, particularly when highly complex systems and multiple products fall within the scope of multiple regulations. Since many organisations already comply with either one or more industry recognised international standards, their adoption and implementation for the purpose of harmonised standards would be efficient from both a standards development and a compliance perspective.

Standards development is a lengthy process. The voices of all participating experts must be heard with the goal of achieving consensus from a multistakeholder community. Standards organisations must also have strong governance that is aligned with the World Trade Organization (WTO) Technical Barriers to Trade (TBT) principles and enforced. More recently, standards bodies have been expected to develop harmonised standards with extremely tight timelines, which has proved challenging for the development of high-quality standards documentation that sufficiently meets expectations to support regulations. Additionally, harmonised standards supporting the CRA should be developed with recognised standards setting organisations in an open, consensus-driven manner through consistent expert multistakeholder engagement. Microsoft therefore also encourages the Commission to provide greater clarity on Article 19 and whether it is intended to allow the Commission without proper and clear legal conditions to draft and implement common specifications.

When harmonised standards are published, a timeline should be provided to all organisations before the regulatory requirements are enforced so organisations can conduct a gap analysis, address additional engineering needs, and comply with the additional requirements. In scope products listed in Annex III are highly complex and can have multiple layers of dependencies and interconnections. Therefore, a minimum of 12 months between the publication of harmonised standards and the expectation to comply would help support meaningful implementation.

Microsoft recommends:

53. Using harmonised standards developed for the CRA and reflecting current cybersecurity best practices, including existing, internationally recognised standards such as the ISO/IEC 27000 series[38] and those from other recognised standards setting organisations such as ETSI[39], CEN CENELEC[40], and NIST, as well as WTO TBT principles that are the result of broad stakeholder engagement and are widely accepted as good practice across industry.
54. Avoiding the use of common specifications by removing Article 19.
55. Allowing a minimum of 12 months between the publication of harmonised standards, common specifications, or cybersecurity certification schemes and the enforcement of requirements to provide enough time for economic operators to effectively comply.

[38] https://www.iso.org/isoiec-27001-information-security.html
[39] https://www.etsi.org/
[40] https://www.cencenelec.eu/

Improving certification through reuse

Cost and scale challenges can be mitigated by promoting global and cross-sector consistency in requirements and reuse of certifications or their conformance artifacts or evidence (e.g., documentation). For example, Common Criteria[41] certifications are recognised by all government members[42] of the Common Criteria Recognition Arrangement.[43] Likewise, there are certifications for globally recognised standards, such as ISO/IEC 27001,[44] involving evaluation of practices that are generally considered foundational to cybersecurity.[45] Applying broadly applicable certifications and standards to the greatest extent possible, then focusing assessments on any requirement gaps helps address resource challenges, reduces diversion of security expertise toward compliance, improves efficiency, and provides greater access to modern technology reflecting the latest security practices.

The CRA proposal envisions that Cybersecurity Act certifications could demonstrate conformity, but greater clarity on how the various levels of assurance may apply is needed. More broadly, leveraging global standards and best practices and the reuse of artifacts and evidence of existing conformance verification processes can expedite the processes of both developing certifications and assessing conformance. Moreover, ensuring certifications can be used seamlessly across the EU's digital single market will help address cost and scale challenges.

Microsoft recommends:

56. Clarifying the level of assurance required. (i.e., basic, substantial, or high) when CRA conformity assessments are based on EU Cybersecurity Act certification schemes.
57. To the greatest extent practicable, enabling, encouraging, and recognising the reuse of existing compliance certifications and materials in the conformity assessment processes used for the CRA.

Defining substantial modification

The concept of "substantial modification" in Recital 23 and Article 3(31) is overly broad and inconsistent with other EU resources. This has implications for manufacturers, importers, and distributors and their obligations within the CRA. Specifically, the Commission's 2022 "Blue Guide"[46] on the implementation of EU product rules introduces three criteria applying to software modifications that can be classified as "substantial":

i) the software update modifies the original intended functions, type or performance of the product and this was not foreseen in the initial risk assessment;

ii) the nature of the hazard has changed or the level of risk has increased because of the software update; and

iii) the product is made available (or put into service where this is covered by the specific Union harmonisation legislation).

[41] https://www.commoncriteriaportal.org/

[42] https://www.commoncriteriaportal.org/ccra/members/

[43] https://www.commoncriteriaportal.org/ccra/

[44] https://www.iso.org/standard/82875.html

[45] Microsoft product groups maintain dozens of certifications for global, government, and industry standards. For example, Azure compliance documentation describes certifications and standards as well as guidance on implementation and control mappings. (Link: https://learn.microsoft.com/en-us/azure/compliance/)

[46] Sec. 2.1. of the Commission notice The "Blue Guide" on the implementation of EU product rules 2022 (Text with EEA relevance) 2022/C 247/01 (Link: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022XC0629%2804%29)

The guide further states that an assessment must be done on a case-by-case basis, taking into consideration the objective of the legislation and the type of products covered by the legislation in question.

Microsoft recommends:

58. Considering the European Commission's Blue Guide to clarify the definition of a "substantial modification" in Recitals 22, 23, 24 and Article 3(31), Article 15, Article 16, and Article 55(2).

Evaluating and communicating conformity

The declaration of conformity should allow for first party and third-party conformity assessment and be consistent with conformity assessment procedures defined by ISO[47] and IEC.[48] Combining declarations as described in Article 20(3) is encouraged to improve the efficiency of compliance for multiple regulatory requirements. Further efficiencies for compliance and declaration activities should be pursued to minimise compliance burdens, availing resources to be focused on improving product features and cybersecurity.

CE marking has generally been required from a safety perspective, but there are important differences between user expectations and readiness required to use products in a way that maintains their safety versus their cybersecurity. Under the CRA, the CE label risks being interpreted as a binary label for cybersecurity by consumers. Consumer labels for products with digital elements should be easy to understand and communicate a clear value proposition, but doing so consistently across vast, complex, and dynamic ICT product categories is challenging. Among well-known consumer labels in other contexts, we anticipate a cybersecurity label for products with digital elements may be more akin to a nutrition label, which benefits from more nuanced consumer interpretation, than an energy efficiency label, which conveys straightforward information about energy use. Just as nutrition decisions are one component of a consumer's efforts to achieve positive health outcomes, in the context of products with digital elements, broader circumstances, including user practices, also impact security risk.

Microsoft recommends:

59. Using conformity assessment procedures consistent with those defined by ISO and IEC.
60. Conducting studies to understand the nuances of using the CE marking to convey cybersecurity properties and combining them with educational campaigns to maximise the value to consumers and organisations.

Making conformity assessment manageable

It is essential that EU Cybersecurity Act certification schemes incorporate the expertise from established conformity assessment bodies. When economic operators are legally required to certify their products in scope of the CRA, it is essential to ensure that EU Cybersecurity Act-based certification requirements are effective and realistic and take a pragmatic approach to ensure that compliance activities are manageable. This is in particular a concern for smaller organisations.

[47] https://www.iso.org/conformity-assessment.html
[48] https://www.iec.ch/conformity-assessment

Additionally, it should be ensured that a CRA certification carried out by one organisation in one member state is recognised by all EU Member States, similar to the EU Cybersecurity Act Certification mutual recognition principle. The certification body which would be granting the certification should have the necessary resources and skills to be able to carry out the assessment in a timely manner. Furthermore, it should be ensured that the points of intersection between the existing regulations and directives such as GDPR or the Directive (EU) 2016/943[49] and the new harmonised standards are highlighted to reduce the compliance burden on organisations and facilitate easier adoption.

Microsoft recommends:

61. Ensuring CRA conformity assessment procedure requirements are effective, realistic, manageable, and consider the impact on smaller organizations.
62. Highlighting intersections between conformity assessment criteria and related regulations and directives when practical.

Market surveillance and enforcement (Chapter 5)

Creating cooperation frameworks for market surveillance authorities

In parallel and coordination with the NIS2 Directive, the CRA lacks a clear mechanism for cooperation between the market surveillance authorities and NCAs in NIS2. To avoid fragmentation and enhance mutual reinforcement between the two EU legislations in the future, and to increase accountability and clarity, how to address these intersections should be proactively considered and regularly revisited.

Microsoft recommends:

63. Creating a workstream for CRA compliance in parallel to or under the NIS Cooperation Group (Article 46(5)).

Delegated powers and committee procedure (Chapter 6)

Consulting and the European Commission's mandate

Stakeholder consultation should accompany the adoption of delegated/implementing acts, including the following envisioned acts:

- Article 2(4) – Delegated act to limit/exclude certain products from application of requirements
- Article 10(15) – Implementing act on SBOM
- Article 23(5) – Delegated act on elements included in technical documentation
- Article 45(4) – Implementing acts to decide on corrective or restrictive measures

Such an approach will help ensure that policy design and gradual implementation considers the ongoing input of economic operators as they prepare to implement CRA requirements.

[49] https://eur-lex.europa.eu/eli/dir/2016/943/oj

Microsoft recommends:

64. Adding “based on the public consultation and relevant stakeholder input, especially economic operators which place their products on the EU market” (for Articles 2(4), 10(15), 23(5), and 45(4), either through changes to Article 50 or elsewhere).

Transitional and final provisions (Chapter 8)

Prioritising cybersecurity workforce development

The EU has proposed several cybersecurity regulations, including two NIS Directives, the Cybersecurity Act, and the Cybersecurity Competence Center and Network Regulation. It has also identified a gap in the EU’s cybersecurity workforce, which challenges efforts to ensure adequate enforcement of proposed legislation. A detailed roadmap and phased approach to implementation should account for these challenges and include efforts to increase readiness of and ensure consistent approaches across market surveillance authorities, ENISA, and conformity assessment bodies.

Microsoft recommends:

65. Adding a prerequisite to applying obligations to manufacturers that ENISA, conformity assessment bodies, and market surveillance authorities demonstrate readiness to fulfil responsibilities, including the consistent validation of operational systems as appropriate (Article 57).

Appendix I – Additional proposal text and comments

Article	Comment	Recommendation
Recital 10	Clarify the intended scope of the open source exclusion and related commercial activity.	Update Recital 10, "In order not to hamper innovation or research, free and open source software should not be covered by this regulation unless it is offered as a paid or monetised product. This is the case for software, including its source code and modified versions, that is openly shared and freely accessible, usable, modifiable and redistributable. Free and open source software development contributes between €65 billion to €95 billion to EU GDP annually according to research by the European Commission and depends on both volunteer and professional contributions from developers in independent, academic, enterprise, and government roles. In the context of software, a paid or monetised product might be characterised not only by charging a price for a product, but also by charging a price for subscriptions to software updates, by providing a software platform through which the manufacturer monetizes other services, or by the use of personal data for reasons other than exclusively for improving the security, compatibility or interoperability of the software. Technical support, consulting services, and financial sponsorships are not products within the scope of this regulation."
Article 10(2) "For the purposes of complying with the obligation laid down in paragraph 1, manufacturers shall undertake an assessment of the cybersecurity risks associated with a product with digital elements and take the	Per Article 1(b) the Regulation lays down: "essential requirements for the design, development and production of products with digital elements, and obligations for economic operators in relation to these products with	Be consistent about whether "planning" is in scope or not.

Article	Comment	Recommendation
outcome of that assessment into account during the planning, design, development, production, delivery and maintenance phases of the product with digital elements with a view to minimising cybersecurity risks, preventing security incidents and minimising the impacts of such incidents, including in relation to the health and safety of users.”	respect to cybersecurity;” which does not include “planning”.	
Article 10(9) "Manufacturers shall ensure that procedures are in place for products with digital elements that are part of a series of production to remain in conformity. The manufacturer shall adequately take into account changes in the development and production process or in the design or characteristics of the product with digital elements and changes in the harmonised standards, European cybersecurity certification schemes or the common specifications referred to in Article 19 by reference to which the conformity of the product with digital elements is declared or by application of which its conformity is verified."	• Without a definition for “part of a series of production” it is unclear what products with digital elements this paragraph applies to. • Cybersecurity risks and mitigations are dynamic. Conformity assessment criteria change over time. • Once products (especially hardware) have been designed it is not practical for manufacturers to continuously remain in compliance with new attack and mitigation techniques or to redesign the product to address new conformance criteria. Product changes become successively more expensive the closer a product is to being placed on the market and thereafter.	• Remove the clause “part of a series of production” or define it. • Provide adequate (e.g., 12 to 48 months, depending on the complexity of products) grace periods prior to new conformance criteria applying, so manufacturers can accommodate a fixed set of requirements during the design phase. • After a product has completed its conformity assessment to be placed on the market, limit manufacturer obligations to risk based security updates based on vulnerability management consistent with the conformance criteria that applied when the product was initially place on the market.

Appendix II – Additional essential cybersecurity requirements and comments

Requirement	Comment	Recommendation
Annex I Section 1(1) "Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks;"	The context that a product is used in has significant bearing on the risks to which it is exposed.	Change "based on the risks" to "based on the risks for intended uses of the product".
Annex I Section 1(2) "Products with digital elements shall be delivered without any known exploitable vulnerabilities;"	• Physical products containing hardware and software are not typically serviced (e.g., updated with security patches) after manufacture and prior to installation by a customer. Rather than requiring physical products be patched before delivery, it should be adequate to deliver products containing known vulnerabilities, provided those vulnerabilities can be patched prior to the product entering into service using an appropriately secured update mechanism. • Annex I Section 1(3)(k) already requires, "ensure that vulnerabilities can be addressed through security updates" and Annex II 9(c) informs users, "how security-relevant updates can be installed" removing the need to pull products placed on the market out of distribution channels to install security updates prior to delivery. • The phrase "without any known exploitable vulnerabilities" is at odds with "appropriate level" and "based on the risks." Some vulnerabilities may be extremely difficult to exploit, may be only exploitable in	Remove the essential cybersecurity requirement in Annex I Section 1(2).

Requirement	Comment	Recommendation
	environments the product is not intended for use in, or may have little or no impact on the product.	
Annex I Section 1(3)(a) "be delivered with a secure by default configuration, including the possibility to reset the product to its original state;"	• What is considered secure may vary depending on the context that a product is used in, however, a manufacturer will need to choose defaults that are appropriate for the typical use of a product. • Fully complying with resetting a product to its original state would require discarding security updates, increasing customer risk; • If the product scope includes remote data processing, the end result of a reset on remote data processing and associated storage is unclear; • Resetting the product to its original state would require discarding security log information. Such a feature would benefit attackers.	Clarify the goal. For example, customers can erase personal data collected during use, assist in recovering the device after a cybersecurity compromise, transfer ownership, etc. Replace with language from NIST IR 8259A[50]: • "The ability for authorized entities to restore the device to a secure configuration defined by an authorized entity," • "The ability for authorised entities to render all data on the device inaccessible by all entities, whether previously authorised or not (e.g., through a wipe of internal storage, destruction of cryptographic keys for encrypted data)".
Annex I Section (3)(c) "protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state-of-the-art mechanisms;"	• The meaning of "otherwise processed data" is not clear. • Some products are designed to use or generate public information. For example, to read and post public messages. The requirement should be modified to protect confidential data (versus all data).	Clarify the meaning of "otherwise processed data". Consider, "protect confidential data when stored, transmitted or processed from unauthorised access, such as by encrypting relevant data at rest or in transit by state-of-the-art mechanisms"

[50] https://csrc.nist.gov/publications/detail/nistir/8259a/final