CEN/CLC/JTC 13/WG 9 "Special Working Group on Cyber Resilience Act"
WG Secretariat: **NEN**
Convenor: **Kokx B. Dhr.**

Second Draft Sreq CRA

Document type	Related content	Document date	Expected action
General / Other		2024-04-18	

Replaces: N 16 CRA draft standardisation request with annexes

EUROPEAN COMMISSION
Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs

Ecosystems III: Construction, Machinery and Standardisation
Standards Policy

Brussels, 16.4.2024

A Notification under Article 12 of Regulation (EU) No 1025/2012[1]

Subject matter related to

☐	Annual Union Work Programme for European standardisation (Art. 12, point a)
☒	Possible future standardisation requests to the European standardisation organisations (Art. 12, point b)
☐	Formal objections to harmonised standards (Art. 12, point c)
☐	Identifications of ICT technical specifications (Art. 12, point d)
☐	Delegated acts to modify Annexes I or III of Regulation (EU) No 1025/2012 (Art. 12, point e)

Title of the initiative

Draft standardisation request to European Standards Organisations in support of Union policy on cybersecurity requirements for products with digital elements

Additional information

Legislative/Policy reference(s)	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, COM/2022/454 final European Parliament legislative resolution of 12 March 2024 on the proposal for a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (COM(2022)0454 – C9-0308/2022 – 2022/0272(COD)), P9_TA(2024)0130
EN reference(s)	-
Status	Draft
Other information	This draft has not been adopted or endorsed by the European Commission. Any views expressed are the preliminary views of the Commission services and may not in any circumstances be regarded as stating an official position of the Commission. The information transmitted is intended only for the Member State or entity to which it is addressed for discussions and may contain confidential and/or privileged material.
Deadline for feedback	16.5.2024

Commission contact point for this notification

CNECT-CRA@ec.europa.eu

[1] OJ L 316, 14.11.2012, p. 12

Brussels, XXX
[…](2024) XXX draft

COMMISSION IMPLEMENTING DECISION

of XXX

on a standardisation request to European Standards Organisations in support of Union policy on cybersecurity requirements for products with digital elements

COMMISSION IMPLEMENTING DECISION

of XXX

on a standardisation request to European Standards Organisations in support of Union policy on cybersecurity requirements for products with digital elements

Version of 16 of April 2024

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council,[1] and in particular Article 10(1) thereof,

Whereas:

(1) On 15 September 2022, the Commission published a proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020.[2] As part of the ordinary legislative process, the co-legislators reached a political agreement in November 2023, as defined in the position of the European Parliament adopted at first reading on 12 March 2024 (hereinafter the "agreed Cyber Resilience Act").

(2) The agreed Cyber Resilience Act aims to ensure that manufacturers take security seriously throughout a product's life cycle. In order to do so, it lays down rules for the placing on the market of products with digital elements and essential requirements for their design, development and production. It also proposes essential requirements for the vulnerability handling processes put in place by manufacturers.

(3) Harmonised standards play an important role in facilitating the assessment of conformity with those requirements. Products with digital elements which are in conformity with harmonised standards, which translate those essential requirements into detailed technical specifications, should therefore be presumed in conformity with the CRA.

(4) Annex I of the agreed Cyber Resilience Act sets forth the essential requirements manufacturers have to demonstrate conformity with, in order to ensure that the

[1] OJ L 316, 14.11.2012, p. 12.
[2] COM(2022) 454.

products they place on the market are secure from a cybersecurity standpoint and that vulnerabilities are handled appropriately.

(5) The presumption of conformity given by harmonised standards or parts thereof is particularly relevant for the products with digital elements listed in Annex III of the agreed Cyber Resilience Act. Products listed in Class I would particularly benefit from harmonised standards since they could remove the obligation to carry out third-party conformity assessment. For products classified under Class II, the existence of harmonised standards would support the development of conformity assessment activities and support market players in ensuring compliance of their products.

(6) To prepare the necessary technical environment for the implementation of the upcoming Cyber Resilience Act it is necessary to develop harmonised European standards and other European standardisation deliverables in the technical areas covered by that Regulation.

(7) The European standards and other standardisation deliverables requested in this Decision are based on discussions with relevant stakeholders which have taken place in the context of the preparation and on-going ordinary legislative procedure of the agreed Cyber Resilience Act.

(8) Given the broad scope of the Cyber Resilience Act, a two-fold approach for developing the standards in response to this request would be appropriate. On the one hand, a set of horizontal standardisation deliverables should provide a coherent generic framework, methodology and taxonomy that can be used to develop further product-specific standards according to market needs. On the other hand, vertical standards are needed, notably as regards the products listed in Annex III of the Cyber Resilience Act, covering a specific set of risks appropriate to a given intended purpose and foreseeable use.

(9) When considering the scope of products under the Cyber Resilience Act for the purposes of the development of horizontal standards, the addressees should, where appropriate, take into consideration that the essential requirements laid down in Annex I of the Cyber Resilience Act will apply to products with digital elements that are also in the scope of different legislative initiatives. These include electronic health record systems under the proposed European Health Data Space Regulation, high-risk AI systems under the AI Act, machinery products under the Machinery Regulation, or trusted chips under the Chips Act.

(10) The addressees should ensure the overall coordination of the activities. Furthermore, they should remain responsible for steering the horizontal work and ensuring good coordination among different technical committees working on the vertical standards. Consultations and other measures to ensure fair and diverse participation in the development of standards should especially target manufacturers of products with digital elements that are small and medium enterprises. Where relevant, particular account should be given to the needs of the free and open source software community.

(11) Aiming to achieve a relevant coverage of intended uses and respective risks, the deliverables prepared in support of this request should be subject to public consultation, aiming to support the standards development work. Attention should be given to ensure the inclusion of European stakeholders in the standardisation process, in particular encouraging the participation of SMEs.

(12) The intention to request the preparation of European standards or European standardisation deliverables in support of the agreed Cyber Resilience Act is stated in point 5 of the table entitled '*Actions for the development and revision of European standards or European standardisation deliverables supporting the strategic priorities*' in the Annex to the Commission Notice on '*The 2023 annual Union work programme for European standardisation*'.[3]

(13) Standards developed at international level by the International Organization for Standardisation (ISO) and the International Electrotechnical Commission (IEC) in relevant areas may be adopted as European standards by CEN and Cenelec on the basis of the Vienna[4] and the Frankfurt[5] agreements. Standards developed by other international consortia may also be considered in the development of the European Standards under this request, provided the legal requirements set out in Regulation (EU) No 1025/2012 are fully met in their development.

(14) There is a large body of existing international standards that are relevant to the scope of this request. Appropriate modes of cooperation between the European Standardisation Organisations, internal cooperation between technical committees, and cooperation with international standardisation organisations should therefore be established to benefit from possible synergies with existing or related European and international standards.

(15) The standards and standardisation deliverables to be developed in response to this request are of strategic importance for the Union. The addressees should ensure that European standards or European standardisation deliverables produced as a result of this request are fully in line with the European legal framework and the EU's objectives and values as set out in Communications *The EU's Cybersecurity Strategy for the Digital Decade (JOIN(2020) 18 final)* and *An EU Strategy on Standardisation – Setting global standards in support of a resilient, green and digital EU single market* (COM(2022) 31 final).

(16) The Commission's Joint Research Centre together with the European Cybersecurity Agency (ENISA) have carried out a mapping of existing international and European standards. This has been shared with the European Standardisation Organisations to initiate a discussion and carry out a detailed gap analysis. In this context, the addressees are encouraged to establish good working relationships with ENISA and the Joint Research Centre as part of the process of development of standards in response to this request.

(17) During the execution of a standardisation request, it may be necessary to adjust the scope of the request or the deadlines set therein. The addressees should therefore promptly report to the Commission if they consider that more time is required to draft the standards or the standardisation deliverables than what was initially foreseen, or that it is necessary to adapt the scope of the request, in order to allow the Commission to take appropriate action.

(18) The addressees have agreed to follow the Guidelines for the execution of standardisation requests[6].

[3] OJ C 93, 13.3.2023, p. 2–31
[4] Agreement on technical cooperation between the ISO and CEN (Vienna Agreement).
[5] IEC-CENELEC Frankfurt Agreement.
[6] SWD(2015) 205 final of 27 October 2015

(19) In order to ensure transparency and facilitate the execution of the requested standardisation activities the addressees should prepare a work programme and submit it to the Commission.

(20) In order to enable the Commission to better monitor the requested standardisation work, the addressees should provide the Commission with access to an overall project plan containing detailed information on the execution of the standardisation request and should report regularly on the execution of that request.

(21) The standards should include detailed technical specifications of the essential cybersecurity requirements, with respect to the design, development and production of products with digital elements as well as to the processes for vulnerability handling. They should also indicate clearly the correspondence between technical specifications and the essential cybersecurity requirements they aim to cover. The addressees should ensure that the developed European Standards and European standardisation deliverables are consistent with the EU legal framework.

(22) In particular, the addressees should take into account, as appropriate, the standardisation work carried out in the context of Commission Implementing Decision C(2022)5637 (RED Delegated Act),[7] Commission Implementing Decision C XXX/XX[8] (AI Act), and also forthcoming standardisation requests such as for the Machinery Regulation, in the preparation and development of requested European standards and European standardisation deliverables. The addressees should also consider any other relevant on-going European standardisation work related to other Union legislation, such as Regulation (EU) XXXX/XX (the Chips Act).

(23) In accordance with Article 10(3) of Regulation (EU) No 1025/2012 each standardisation request is subject to acceptance by the relevant European standardisation organisation. It is therefore necessary to provide for the rules on validity of this request if it is not accepted by the addressees.

(24) In order to ensure legal certainty as to the validity of the request after its execution, it is appropriate to provide for a date of expiry of this Decision.

(25) The European standardisation organisations, the European stakeholders' organisations receiving Union financing and the Member States experts in the Multi-stakeholder Platform on ICT standardisation have been consulted.

(26) The measures provided for in this Decision are in accordance with the opinion of the Committee established by Article 22 of Regulation (EU) No 1025/2012.

[7] COMMISSION IMPLEMENTING DECISION on a standardisation request to the European Committee for Standardisation and the European Committee for Electrotechnical Standardisation as regards radio equipment in support of Directive 2014/53/EU of the European Parliament and of the Council and Commission Delegated Regulation (EU) 2022/30

[8] Commission Implementing Decisions C …. [here full title]

HAS ADOPTED THIS DECISION:

Article 1
Requested standardisation activities

The addressees are requested to draft new or revise existing European standards or European standardisation deliverables, as listed in Annex I to this Decision, in support of the agreed Cyber Resilience Act by the deadlines set out in that Annex.

The European standards or European standardisation deliverables referred to in paragraph 1 shall meet the requirements set out in Annex II to this Decision.

Article 2

Work programme

The addressees shall prepare a work programme indicating all the European standards or European standardisation deliverables listed in Annex I of this Decision, the responsible technical bodies and a timetable for the execution of the requested standardisation activities in the terms of article 1 of this Request and in line with the deadlines set out in Annex I to this Decision.

The work programme shall also include the actions to be undertaken to ensure effective participation of relevant stakeholders, such as small and medium enterprises and civil society organisations, including specifically the open source community where relevant, in accordance with Article 5 of Regulation (EU) No 1025/2012.The addressees shall submit the draft work programme to the Commission by *2 months* after the notification of this Decision by the Commission.

The addressees shall inform the Commission of any amendments to the work programme.

The addressees shall provide the Commission with access to an overall project plan.

Article 3
Reporting

The addressees shall report every six months to the Commission on the execution of the request referred to in Article 1, indicating the progress made in the implementation of the work programme referred to in Article 2.

The addressees shall submit the first joint semestrial report to the Commission by 10 months after the notification of this Decision by the Commission. Subsequent joint semestrial reports shall be submitted every six months.

The addressees shall provide the Commission with the joint final report by 30 November 2027.

The addressees shall promptly report to the Commission any major concerns relating to the scope of the request referred to in Article 1 and the deadlines set out in Annex I to this Decision.

The reports referred to in paragraphs 1 to 3 shall include evidence of how the addressees have:

(a) Facilitated representation and participation of the relevant stakeholders, including small and medium enterprises and societal stakeholders, including specifically the open source community where relevant, in accordance with Article 5 of Regulation (EU) No 1025/2012;

(b) Ensured that European standards and European standardisation deliverables are in conformity with Union law on fundamental rights and Union data protection law, in accordance with Annex II.

Article 4
Validity of the standardisation request

Where, in accordance with Article 10(3) of Regulation (EU) No 1025/2012, the addressees indicate that they do not accept the request referred to in Article 1 of this Decision, this request shall not serve as a basis for the standardisation activities referred to in Article 1 of this Decision for the standardisation request concerned.

This Decision shall expire on 30 November 2027.

Done at Brussels,

For the Commission
[…]

(PE/PO/PH)
The President (choose the correct position)
Vice-President (choose the correct position)
Member of the Commission (choose the correct position)

ANNEXES

to the

COMMISSION IMPLEMENTING DECISION

on a standardisation request to European Standards Organisations in support of Union policy on cybersecurity requirements for products with digital elements

ANNEX I

List of new European Standards and/or European standardisation deliverables to be drafted

Reference information		Deadline for the adoption by the ESOs
Horizontal standards for security requirements relating to the properties of products with digital elements		
1.	European standard(s) and/or European standardisation deliverable(s) on designing, developing and producing products with digital elements in such a way that they ensure an appropriate level of cybersecurity based on the risks	30/08/2026
2.	European standard(s) and/or European standardisation deliverable(s) on making products with digital elements available on the market without known exploitable vulnerabilities	30/10/2027
3.	European standard(s) and/or European standardisation deliverable(s) on making products with digital elements available on the market with a secure by default configuration	30/10/2027
4.	European standard(s) and/or European standardisation deliverable(s) on ensuring that vulnerabilities in products with digital elements can be addressed through security updates	30/10/2027
5.	European standard(s) and/or European standardisation deliverable(s) on ensuring protection of products with digital elements from unauthorised access and reporting on possible unauthorised access	30/10/2027
6.	European standard(s) and/or European standardisation deliverable(s) on protecting the confidentiality of data stored, transmitted or otherwise processed by a product with digital elements	30/10/2027
7.	European standard(s) and/or European standardisation deliverable(s) on	30/10/2027

	protecting the integrity of data, commands, programs by a product with digital elements, and its configuration against any manipulation or modification not authorised by the user, as well as reporting on corruptions	
8.	European standard(s) and/or European standardisation deliverable(s) on processing only personal or other data that are adequate, relevant and limited to what is necessary in relation to the intended purpose of the product with digital elements (‘minimisation of data’)	30/10/2027
9.	European standard(s) and/or European standardisation deliverable(s) on protecting the availability of essential and basic functions of the product with digital elements	30/10/2027
10.	European standard(s) and/or European standardisation deliverable(s) on minimising the negative impact of a product with digital elements or its connected devices on the availability of services provided by other devices or networks	30/10/2027
11.	European standard(s) and/or European standardisation deliverable(s) on designing, developing and producing products with digital elements with limitted attack surfaces	30/10/2027
12.	European standard(s) and/or European standardisation deliverable(s) on designing, developing and producing products with digital elements that reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques	30/10/2027
13.	European standard(s) and/or European standardisation deliverable(s) on providing security related information by recording and/or monitoring relevant internal activity of products with digital elements with an opt-out mechanism for the user	30/10/2027

14.	European standard(s) and/or European standardisation deliverable(s) on securely and easily removing or transferring all data and settings of a product with digital elements.	30/10/2027
Horizontal standards for vulnerability handling requirements		
15.	European standard(s) and/or European standardisation deliverable(s) on vulnerability handling for products with digital elements	30/08/2026
Vertical standards for security requirements relating to the properties of products with digital elements		
16.	European standard(s) and/or European standardisation deliverable(s) on essential cybersecurity requirements for identity management systems and privileged access management software and hardware, including authentication and access control readers, including biometric readers	30/10/2026
17.	European standard(s) and/or European standardisation deliverable(s) on essential cybersecurity requirements for standalone and embedded browsers	30/10/2026
18.	European standard(s) and/or European standardisation deliverable(s) on essential cybersecurity requirements for password managers	30/10/2026
19.	European standard(s) and/or European standardisation deliverable(s) on essential cybersecurity requirements for software that searches for, removes, or quarantines malicious software	30/10/2026
20.	European standard(s) and/or European standardisation deliverable(s) on essential cybersecurity requirements for products with digital elements with the function of virtual private network (VPN)	30/10/2026
21.	European standard(s) and/or European standardisation deliverable(s) on essential cybersecurity requirements for network management systems	30/10/2026

22.	European standard(s) and/or European standardisation deliverable(s) on essential cybersecurity requirements for Security information and event management (SIEM) systems	30/10/2026
23.	European standard(s) and/or European standardisation deliverable(s) on essential cybersecurity requirements for boot managers	30/10/2026
24.	European standard(s) and/or European standardisation deliverable(s) on essential cybersecurity requirements for public key infrastructure and digital certificate issuance software	30/10/2026
25.	European standard(s) and/or European standardisation deliverable(s) on essential cybersecurity requirements for physical and virtual network interfaces	30/10/2026
26.	European standard(s) and/or European standardisation deliverable(s) on essential cybersecurity requirements for operating systems	30/10/2026
27.	European standard(s) and/or European standardisation deliverable(s) on essential cybersecurity requirements for routers, modems intended for the connection to the internet, and switches	30/10/2026
28.	European standard(s) and/or European standardisation deliverable(s) on essential cybersecurity requirements for microprocessors with security-related functionalities	30/10/2026
29.	European standard(s) and/or European standardisation deliverable(s) on essential cybersecurity requirements for microcontrollers with security-related functionalities	30/10/2026
30.	European standard(s) and/or European standardisation deliverable(s) on essential cybersecurity requirements for application specific integrated circuits (AS IC) and field-programmable gate arrays (FPGA) with security-related	30/10/2026

	functionalities	
31.	European standard(s) and/or European standardisation deliverable(s) on essential cybersecurity requirements for smart home general purpose virtual assistants	30/10/2026
32.	European standard(s) and/or European standardisation deliverable(s) on essential cybersecurity requirements for smart home products with security functionalities, including smart door locks, security cameras, baby monitoring systems and alarm systems	30/10/2026
33.	European standard(s) and/or European standardisation deliverable(s) on essential cybersecurity requirements for Internet connected toys covered by Directive 2009/48/EC that have social interactive features (e.g. speaking or filming) or that have location tracking features	30/10/2026
34.	European standard(s) and/or European standardisation deliverable(s) on essential cybersecurity requirements for personal wearable products to be worn or placed on a human body that have a health monitoring (such as tracking) purpose and to which Regulation (EU) 2017/745 or Regulation (EU) 2017/746 do not apply or personal wearable products that are intended for the use by and for children	30/10/2026
35.	European standard(s) and/or European standardisation deliverable(s) on essential cybersecurity requirements for hypervisors and container runtime systems that support virtualised execution of operating systems and similar environments	30/10/2026
36.	European standard(s) and/or European standardisation deliverable(s) on essential cybersecurity requirements for firewalls, intrusion detection and/or prevention systems, including specifically those intended for industrial use	30/10/2026
37.	European standard(s) and/or European standardisation deliverable(s) on essential	30/10/2026

	cybersecurity requirements for tamper-resistant microprocessors	
38.	European standard(s) and/or European standardisation deliverable(s) on essential cybersecurity requirements for tamper-resistant microcontrollers	30/10/2026
39.	European standard(s) and/or European standardisation deliverable(s) on essential cybersecurity requirements for Hardware Devices with Security Boxes	30/10/2026
40.	European standard(s) and/or European standardisation deliverable(s) on essential cybersecurity requirements for smart meter gateways within smart metering systems as defined in Article 2 (23) of Directive (EU) 2019/944 and other devices for advanced security purposes, including for secure cryptoprocessing	30/10/2026
41.	European standard(s) and/or European standardisation deliverable(s) on essential cybersecurity requirements for smartcards or similar devices, including secure elements	30/10/2026

ANNEX II

Requirements for the European standards and European standardisation deliverables referred to in Article 1

1. Requirements for all European standards and European standardisation deliverables

European standards and European standardisation deliverables shall reflect the generally acknowledged state of the art[1] in order to minimise the cybersecurity risks which arise in the planning, design, development, production, delivery and maintenance of products with digital elements, aiming to prevent security incidents and minimise the impacts of such incidents, including in relation to the health and safety of users. Product with digital elements means any software or hardware product and its remote data processing solutions, including software or hardware components to be placed on the market separately.

The European standards and European standardisation deliverables shall provide, to the extent necessary and reflecting the state of the art, technology-, process- or methodology-based technical specifications in relation to the design and development of products with digital elements, including evaluation procedures such as testing and review and, to the extent feasible, objectively verifiable criteria and implementable methods to assess compliance with such specifications. When laying down specifications that are relevant for conformity assessment activities, whether by the manufacturer in self-assessment or by a third-party, the addressees shall take into account the following modules of conformity assessment as set out in [Annex VI of the Cyber Resilience Act]: conformity based on internal control, EU-type examination, internal production control and full quality assurance.

The list of standards identified in Annex I should not be seen as overly prescriptive of the technical work that should be carried out by the European Standardisation Organisations. The addressees are free to organise the technical work in order to ensure adequate efficiencies in the process, and may refer to clauses or sub-clauses of a standard in response to this request for any given item, provided the content meets the essential requirements in question. Supporting specifications (e.g. on terminology[2]) should also be identified and provided when necessary to ensure the consistency and implementability of the European standards and European standardisation deliverables. Such supporting documents may also include elements useful for the horizontal framework, such as threat and vulnerability catalogues.

Without prejudice to needed improvements, the standards developed in response to this request should build on the work currently under development to support the Radio Equipment Directive Delegated Regulation 2022/30[3]. The specificities of the Cyber Resilience Act must however be fully addressed during the development stage. Where possible, [ESOs] are encouraged to update already existing standards and standardisation deliverables to align with the requirements of the CRA.

---

[1] The state of the art does not necessarily imply the latest scientific research still in an experimental stage or with insufficient technological maturity. The state-of-the-art is not to be intended as minimum requirements to access the market.

[2] All the European Standards and European standardisation deliverables elaborated on the basis of this request shall rely on a common set of terms. Moreover, supporting specifications on terminology shall build as much as possible on terminology adopted at international level and notably in international standards.

[3] Commission Implementing Decision C(2022)5637 on a standardisation request for the RED Delegated Regulation 2022/30.

The addressees should ensure that the European standards and European standardisation deliverables produced are consistent with the Cyber Resilience Act and when applicable, with other European and harmonised standards developed or under development in the various relevant sectors, notably those related to products covered by existing EU safety legislation, such as the Machinery Regulation, the AI Act and Chips Act, or EU cybersecurity certification schemes developed or under development under Regulation (EU) 2019/881.

Each European standard and European standardisation deliverable produced shall clearly indicate its scope, the products which fall under its scope, and which risks are covered (if applicable). Where a European standard and European standardisation deliverable does not cover all the essential requirements which are applicable to the products falling under its scope, it shall indicate the essential requirements not covered. Where a European Standard and European standardisation deliverable does not mitigate major risks identified after a comprehensive analysis, which relate to one of the essential requirements it aims to cover and which apply to the products falling under its scope, the standard shall indicate the major risks not mitigated and provide, to the extent possible, indications on how else such risks could be addressed.

Such standards should include at least provisions related to the security problem definition, security objectives, technical specification of security requirements, assessment methodology, and guidance for conformity assessment covering the conformity assessment modules as defined in the CRA.

In terms of security problem definition, the standard should be transparent as to the threats it covers, the policies and assumptions it is based on, and should provide guidance to manufacturers on the identification and specification of threats, policies and assumptions. This could for instance be achieved through the development or referencing of existing catalogues of threats and vulnerabilities, and a discussion on reasonable assumptions.

The security objectives should define the scope and the security properties that the target product or service is intended to address, based on the essential requirements defined in the CRA. The statements must concisely express the intended solution to the identified risks (security problem). The method used to identify the security objectives should rely on existing standards defining risk analysis approaches. The standard is expected to include the relation between the security objectives and the identified risks (security problem).

The specification of security requirements describes the desired cybersecurity behaviour expected for the target product or service. Where feasible, the standard should cover a variety of security levels catering to different expected market needs, such as different intended purposes, operational environments or categories of users (e.g. consumer, enterprise, critical).

The assessment methodology shall consist of a set of evaluation procedures required to assess the target against the technical specification requirements identified previously. It defines “how” to evaluate the target to prove the required level of security. It should cover at least the definition of the concept of evaluation methodology, definition of the concept of composition methodology (when relevant), and definition of the expected evaluation results. Additionally, when drafting such provision, the standards shall take into account all the conformity assessment modules defined in the CRA.

Guidance (informative) on requirements for conformity assessment shall describe the requirements for any organisation certifying or self-certifying the target products. In particular, the standard must cover the conformity assessment modules as defined in the CRA.

All standards developed under this request should be drafted in such a way that they may be published in the Official Journal or the EU for potential harmonisation.

2. Requirements for specific European Standards and European standardisation deliverables

2.1 Horizontal cybersecurity standardisation deliverables relating to the properties of products with digital elements (1-15)

The development of horizontal standards addressing different aspects and mechanisms of product cybersecurity can support the coherent development of subsequent vertical standards for products or categories of products. Such horizontal standards must support both the development of further granular vertical standards for specific products or product types, as well as support manufacturers in directly defining security requirements applicable to their respective products. Vertical standards developed under this request shall therefore build on and further specify the horizontal provisions, and wherever needed simply justify deviations.

The first requested item (1) European standard or standardisation deliverable should serve as a framework covering all elements defined in section 1 of this Annex, and shall set out specifications for the design, development and production of products with digital elements in such a way that they ensure an appropriate level of cybersecurity based on the risks.

The remaining horizontal standards (2-15) should be developed taking into account the essential requirements as defined in the agreed CRA (Annex I) and the scope of products with digital elements covered. Rather than focus only on the minimum common aspects, the horizontal standards should strive to provide a broad and useful overview of the specified aspects that can cover the scope of products under the CRA and, wherever relevant, should include provisions on secure software development. The standard should therefore ensure clarity on the scope of each statement.

When considering the scope of products under the CRA for the purposes of the development of horizontal standards, the addressees shall where appropriate take into consideration that the essential requirements laid down in Annex I of the Cyber Resilience Act will apply to products with digital elements that are also in the scope of different legislative initiatives, such as electronic health record systems under the [proposed European Health Data Space Regulation], high-risk AI systems under the [AI Act], machinery products under the [Machinery Regulation], or trusted chips under the [Chips Act].

2.2 Vulnerability handling requirements for products with digital elements (16)

This (these) European standard(s) or European standardisation deliverable(s) shall provide specifications for vulnerability handling processes, covering all relevant product categories, to be put in place by manufacturers of the products with digital elements. Those processes shall at least allow the manufacturer to:

(a) identify and document vulnerabilities and components contained in the product, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the product;

(b) in relation to the risks posed to the products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates; where technically feasible, new security updates shall be provided separately from functionality updates;

(c) apply effective and regular tests and reviews of the security of the product with digital elements;

(d) once a security update has been made available, share and publicly disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and clear and accessible information helping users to remediate the vulnerabilities; in duly justified cases, where manufacturers consider the security risks of publication to outweigh the security benefits, they may delay making public information regarding a fixed vulnerability until after users have been given the possibility to apply the relevant patch;

(e) put in place and enforce a policy on coordinated vulnerability disclosure;

(f) take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third party components contained in that product, including by providing a contact address for the reporting of the vulnerabilities discovered in the product with digital elements;

(g) provide for mechanisms to securely distribute updates for products with digital elements to ensure that vulnerabilities are fixed or mitigated in a timely manner, and, where applicable for security updates, in an automatic manner;

(h) ensure that, where security updates are available to address identified security issues, they are disseminated without delay and, unless otherwise agreed between manufacturer and business user in relation to a tailor-made product with digital elements, free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken.

This (these) European standard(s) or European standardisation deliverable(s) shall be drafted in such as way that would ensure that the harmonised standards may provide presumption of conformity regarding the implementation of appropriate procedures that can support an adequate vulnerability handling, containing at least the elements described above.

2.3 Vertical cybersecurity standardisation deliverables relating to the properties of products with digital elements (17-41)

These European standards or European standardisation deliverables shall provide specifications for the cybersecurity requirements of important or critical products as identified in Annex I of this Request (17-41) and defined in CRA [Annex III] and [IIIa].

Vertical standards shall implement and further develop the provisions of the horizontal framework developed under this Request, set out in Annex I standards 1 to 15 and further described in section 1 and 2.1 of this Annex, while taking also into consideration relevant differences arising from intended purpose and reasonably foreseeable use.

For those products covered in [Annex IIIa of the CRA] for which technical domains or protection profiles exist, the developed standardisation deliverables shall take into account existing EU cybersecurity certification schemes developed or under development under Regulation (EU) 2019/881, in particular the European Common Criteria-based cybersecurity certification scheme (EUCC).

In terms of conformity assessment procedures, the vertical standards developed for this request (17-41) focusing specifically on products subject to third party conformity assessment (important or critical products) shall set forth a risk-based approach to assurance such that lower risk use cases may be subject to validation procedures only, but higher risk use cases would be subject to (increasingly) higher forms of verification procedures.

These European standards shall be drafted in such as way that would ensure that they may provide presumption of conformity with the CRA regarding the sets of risks they identify, and should strive to adequately cover all major risks identified for a given intended purpose or reasonably foreseeable use, and should therefore be based on a comprehensive risk analysis carried out in the development of each standard.

In addition, the development of vertical standards covering a broad scope of products / product categories (such as, among others, for operational technology), may support and facilitate the structured and coherent development of product-specific vertical standards as referred in this Request that can provide a legal presumption of conformity to the CRA, as long as there is no ambiguity on the requirements or the scope. Such broad verticals shall cover the risks that could be identified by a manufacturer considering a concrete intended purpose and reasonably foreseeable use. Such broad vertical standards would also be expected to support the development of further, more granular vertical standards which would aim to provide such presumption of conformity for a more reduced scope.