MITRE Software and Supply Chain Assurance Fall Forum 2023
McLean VA, 12 Sep 2023, V1.1

Deconstruction and Implementation of the EU Cyber Resilience Act (CRA)

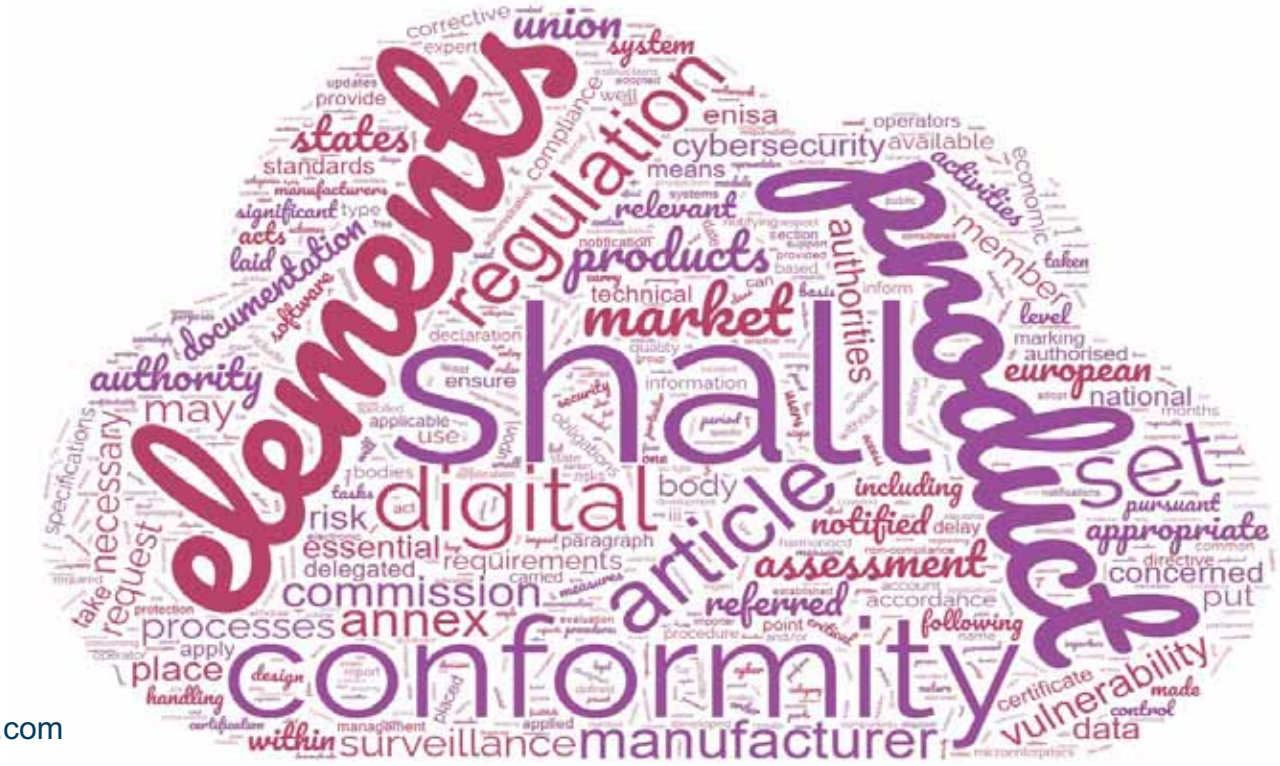
Tony.Rutkowski@CISecurity.org

Disclaimer: the views expressed are those of the author and not necessarily those of CIS or any body with which he is affiliated

Summary

- **The European Union is a supernational governmental authority comprised by 27 Member States consisting of legislative and executive branches (European Commission)**
- **The CRA is the pinnacle of over 400 legislative/regulatory enactments on Information and Communication Technology (ICT) adopted by the Union over the past several years**
- **The CRA text is still draft, but near completion, and subject of negotiations**
- **CRA objectives include**
  - Improve cybersecurity in the EU
  - Pursue “EU technological sovereignty” and “global cybersecurity leadership”
  - Assert EU legal sovereignty over all physical and software “products with digital elements” including remote processes made available in the EU
  - Impose hundreds of onerous certification, testing, notification, reporting, and support requirements and standards on all manufacturers, distributors, and importers of such products, including their components, versions and variants
- **The CRA arguably is the most far reaching, impactful, harmful, and misguided set of actions ever taken in the cybersecurity domain by a major governmental authority**
- **Creates numerous undesirable precedents, and poses significant national and cyber security threats and challenges to U.S. and its industry, ref. ONCD RFI Q9 https://www.regulations.gov/document/ONCD_FRDOC_0001-0002**

EU Cyber Resilience Act



Credit: wordcloud.com

CRA basics

- Formally - *REPORT 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*, ELI: https://www.europarl.europa.eu/doceo/document/A-9-2023-0253_EN.html
- Exists as a companion to the NIS2 Directive, Critical Entities Resilience (CRE) Directive, Digital Operational Resilience Directive (DORA), and Product Market Surveillance Act
- Latest European Parliament revised version submitted to European Commission, 26 Jul 2023
- Expansive, complex cybersecurity regulatory mandates to "raise the overall level of cybersecurity in the Member States and the functioning of the internal market," "legal clarity," and "to ensure that the Union can play a leading role in the definition of norms on cybersecurity on the global stage"
- Establishes extensive conformance requirements and procedures for all "products with digital elements" and associated obligations on all manufacturers, importers, or distributors
- Focuses initially on 40 product sectors with several provisions to significantly expand provisions and reach
- Creates new EU implementation bodies and administrative mechanisms
- Regulations are implemented through extensive impositions on Member States, including certification, surveillance and other enforcement measures combined with large penalties imposed on product non-conformance or "economic operator" non-compliance with the obligations
- Relies on using "harmonised standards" from 3 ESOs (CEN, CENELEC, ETSI), "taking into account existing or imminent international standards" for cybersecurity from 3 ISOs (ISO, IEC, or ITU)
- Comes into force 20th day after publication, and applies 3 years afterward
- ESOs tentatively required to submit draft regulatory standards by 31 May 2026

CRA Provisions

CRA Annexes

ANNEX I ESSENTIAL CYBERSECURITY REQUIREMENTS

1. Security requirements relating to the properties of products with digital elements (15 requirements)
2. Vulnerability handling requirements (9 requirements)

ANNEX II INFORMATION AND INSTRUCTIONS TO THE USER (12 requirements)

ANNEX III CRITICAL PRODUCTS WITH DIGITAL ELEMENTS

Class I

1. Identity management systems software and privileged access management software
2. Standalone and embedded browsers
3. Password managers

3a. Biometric readers

4. Software that searches for, removes, or quarantines malicious software
5. Products with digital elements with the function of virtual private network (VPN)
6. Network management systems
7. Network configuration management tools
8. Network traffic monitoring systems
9. Management of network resources
10. Security information and event management (SIEM) systems
11. Update/patch management, including boot managers
12. Application configuration management systems
13. Remote access software
14. Mobile device management software
15. Physical and virtual network interfaces
16. Operating systems not covered by class II
17. Firewalls, intrusion detection and/or prevention systems not covered by class II
19. General purpose microprocessors and microprocessors not covered by class II
20. Microcontrollers
21. Application specific integrated circuits (ASIC) and field-programmable gate arrays (FPGA) intended for the use by essential entities (ref. Art. 3 of Directive(EU) 2022/2555)
22. Industrial Automation & Control Systems (IACS) not covered by class II, such as programmable logic controllers (PLC), distributed control systems (DCS), computerised numeric controllers for machine tools (CNC), industrial robots and their control systems and supervisory control and data acquisition systems (SCADA)
23. Industrial Internet of Things not covered by class II

23a. Home automation systems, including smart home servers and virtual assistants

23b. Security devices, including smart door locks, cameras and alarm systems

23c. Smart toys

23d. Personal health appliances and wearables

ANNEX III CRITICAL PRODUCTS WITH DIGITAL ELEMENTS

Class II

1. Operating systems for servers, desktops, and mobile devices
2. Hypervisors and container runtime systems that support virtualised execution of operating systems and similar environments
3. Public key infrastructure and digital certificate issuers
4. Firewalls, intrusion detection and/or prevention systems intended for industrial use
6. Microprocessors intended for integration in programmable logic controllers and secure elements
7. Routers, modems intended for the connection to the internet, and switches
8. Secure elements;
9. Hardware Security Modules (HSMs)
10. Secure cryptoprocessors
11. Smartcards, smartcard readers and tokens
12. Industrial Automation & Control Systems (IACS) intended for the use by essential entities of the type referred to in Article 3 of Directive (EU) 2022/2555, such as programmable logic controllers (PLC), distributed control systems (DCS), computerised numeric controllers for machine tools (CNC) and supervisory control and data acquisition systems (SCADA)
13. Industrial Internet of Things devices intended for the use by essential entities of the type referred to in Article 3 of Directive (EU) 2022/2555;
15. Smart meters

ANNEX IV EU DECLARATION OF CONFORMITY (8 requirements)

ANNEX V CONTENTS OF THE TECHNICAL DOCUMENTATION (12 requirements)

ANNEX VI CONFORMITY ASSESSMENT PROCEDURES

Module A: Conformity Assessment procedure based on internal control
Module B: EU-type examination
Module C: Conformity to type based on internal production control
Module H: Conformity based on full quality assurance

ANNEX VIa CAPACITY NEEDS OF ENISA

Annex VI Conformity assessment modules

- **Module A: Conformity Assessment procedure based on internal control**
  - Where the manufacturer fulfils the obligations laid down and ensures and declares on its sole responsibility that the products with digital elements satisfy all the essential requirements set out in Section 1 of Annex I and the manufacturer meets the essential requirements set out in Section 2 of Annex I
- **Module B: EU-type examination**
  - Where a notified body examines the technical design and development of a product and the vulnerability handling processes put in place by the manufacturer, and attests that a product with digital elements meets the essential requirements set out in Section 1 of Annex I and that the manufacturer meets the essential requirements set out in Section 2 of Annex I
- **Module C: Conformity to type based on internal production control**
  - Where the manufacturer fulfils the obligations laid down and ensures and declares that the products concerned are in conformity with the type described in the EU-type examination certificate and satisfy the essential requirements set out in Section 1 of Annex I
- **Module H: Conformity based on full quality assurance**
  - Where the manufacturer fulfils the obligations laid down and ensures and declares on his sole responsibility that the products (or product categories) concerned satisfy the essential requirements set out in Section 1 of Annex I, and that the vulnerability handling processes put in place by the manufacturer meet the requirements set out in Section 2 of Annex I

CRA institutional components

Standards Bodies

- ITU *
- ETSI
- ISO *
- IEC *
- CEN
- CENELEC

Economic Operators

- Manufacturer
- Authorised Representative
- Distributor
- Developer
- Importer
- Natural or legal person

EU Member States

- Market Surveillance Authority
- Notifying Authority
- CSIRT
- National Accreditation Body
- National authority responsible for notification policy

EU Institutions

- European Commission
- ENISA
- CRA Dedicated Administrative Cooperation Group (ADCO)
- EC CRA Committee
- EU-CyCLONe
- European Data Protection Board
- Expert Group on Cyber Resilience
- European Cybersecurity Competence Centre

- Conformity Assessment Body
- Micro enterprise
- Small enterprise
- Consumer
- Medium Size enterprise

Mutual Recognition Agreement Country

* Shall strive to take into account per Art. 18

CRA purpose and subject matter (Art. 1)

- **Establishes**
  - rules for the making available on the market of *products with digital elements* to ensure their cybersecurity (147 occurrences)
  - *essential requirements* for the design, development and production of *products with digital elements*, and obligations for economic operators in relation to these products with respect to cybersecurity
  - *essential requirements* for the vulnerability handling processes put in place by manufacturers to ensure the cybersecurity of *products with digital elements* during the whole life cycle, and obligations for economic operators for these processes
  - rules on market monitoring, surveillance and enforcement of the CRA rules and requirements

CRA Scope (Art. 2)

- **Includes**
  - *products with digital elements* made available on the market that can have a direct or indirect data connection to a device or network
    - six subcategories defined: critical product (Art. 3 & Annex III), highly critical product (Arts. 3; 6); product presenting a significant cybersecurity risk (Arts. 43-46); product classified as high-risk AI system (Art. 8); machinery product (Art. 9); public procurement product (Art. 9a)
- **Excludes**
  - free and open-source software where such software is made available on the market in the course of non-commercial activity
  - products with digital elements subject to EU Regulations for
    - sale of medical devices for human use
    - in vitro diagnostic medical devices
    - motor vehicles, their trailers, systems, components, technical units
    - certified under aviation safety rules
  - products with digital elements covered by other Union rules laying down requirements that address all or some of the risks covered by the essential requirements and achieve the same level of protection
  - products developed exclusively for national security or military purposes or specifically designed to process classified information
  - product spare parts that are exclusively manufactured to replace identical parts and that are supplied by the manufacturer of the original products

Significant CRA definitions (Art.3)

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

remote data processing: means any data processing at a distance for which the software is designed and developed by or on behalf of the manufacturer, and the absence of which would prevent the product with digital elements from performing one of its functions

critical product with digital elements: means a product with digital elements that presents a cybersecurity risk in accordance with the criteria laid down in Article 6(2) and whose core functionality is set out in Annex III

highly critical product with digital elements: means a product with digital elements that presents a cybersecurity risk in accordance with the criteria laid down in Article 6(5)

economic operator: the manufacturer, the authorised representative, the importer, the distributor, or any other natural or legal person who is subject to obligations laid down by this Regulation

manufacturer: any natural or legal person who develops or manufactures products [or a substantial modification] with digital elements or has products with digital elements designed, developed or manufactured, and markets them under his or her name or trademark, whether for payment, monetisation or free of charge

making available on the market: any supply of a product with digital elements for distribution or use on the Union market in the course of a commercial activity, whether in return for payment or free of charge

importer: any natural or legal person established in the Union who places on the market a product with digital elements that bears the name or trademark of a natural or legal person established outside the Union

distributor: any natural or legal person in the supply chain, other than the manufacturer or the importer, that makes a product with digital elements available on the Union market without affecting its properties

substantial modification: a change to the product with digital elements following its placing on the market, which affects the compliance of the product with digital elements with the essential requirements set out in Section 1 of Annex I or results in a modification to the intended use for which the product with digital elements has been assessed, excluding necessary security updates that aim to mitigate vulnerabilities

international standard: an international standard adopted by the International Organisation for Standardisation (ISO), the International Electrotechnical Commission (IEC) or the International Telecommunication Union (ITU)

General Provisions (Chap. I)

- **Free Movement (4)**
  - Member States shall not impede compliant products nor prototypes for testing
- **Requirements for products with digital elements (5)**
  - Products shall only be made available on the market where they meet Annex 1 essential requirements and processes, and installed, maintained and used in their intended environment
- **Critical products with digital elements (6)**
  - Critical products listed in Annex III, with Class I and Class II reflecting the level of risk, will be evolved per 8 described attributes, and subject to specified conformity assessment procedures
  - The EC is empowered to designate “highly critical products” for which a conformance certificate and specifications for a “high assurance level”
- **Expert Group on cyber resilience (6a)**
  - The EC shall establish an expert group on cyber resilience that shall advise on the Annex III list of critical products and other elements of the CRA
- **Enhancing skills in a cyber resilient digital environment (6b)**
  - The EC and Member States shall implement education and training programmes in the cyber security field and enhance collaboration
- **General product safety (7)**
  - Products not subject to specific CRA requirements may be required to meet other EU general product safety regulations
- **High-risk AI systems (8)**
  - Products classified as high-risk AI Systems under the AI Act must meet specified Annex I requirements, with the AI Act still applying.
- **Machinery products (9)**
  - Defines the conformity cybersecurity requirements for products falling under the EU Machinery and Equipment Regulation
- **Public procurement of products with digital elements (9a)**
  - Member States shall ensure procured products have a high level of cybersecurity and remedy vulnerabilities

Obligations of Economic Operators (Chap. II)

- **Obligations of manufacturers (10)**
  - When placing a product with digital elements on the market, manufacturers shall comply with 27 requirements
- **Reporting obligations of manufacturers (11)**
  - Manufacturer shall notify ENISA within 24 hours of any active exploited vulnerability contained in the product with any corrective or mitigating measures, and complying with six requirements
  - Manufacturer shall notify ENISA within 72 hours of any significant incident having impact on the security of the product with any corrective or mitigating measures, and complying with twelve requirements
  - Manufacturer shall notify users without undue delay of any significant incident having impact on the security of the product with any corrective or mitigating measures, and complying with twelve requirements
- **Voluntary notification (11a)**
  - Six processes specified for reporting incidents, cyberthreats and near misses to ENISA
- **Point of single contact for users (11b)**
  - Manufactures will establish and make public a single point of contact and means of contact for users
- **Authorised representatives (12)**
  - A manufacturer may appoint an authorised representative for certain purposes subject to six conditions
- **Obligations of importers (13)**
  - Importers shall only place on the market products with digital elements that comply with the essential requirements set out in Section 1 of Annex I, and comply with 13 requirements
- **Obligations of distributors (14)**
  - Distributors shall only place on the market products with digital elements that comply with 8 requirements
- **Cases in which obligations of manufacturers apply to importers and distributors (15)**
  - If importer or distributor uses own name or modifies the product, they are treated as a manufacturer
- **Other cases in which obligations of manufacturers apply (16)**
  - If any natural or legal person modifies a product they are treated as a manufacturer
- **Identification of economic operators (17)**
  - Shall be able to supply for ten years the name and address of all their suppliers and economic operators to whom they have been a supplier
- **Guidelines (17a)**
  - EC will produce guidelines for economic operators how to implement the CRA

Conformity of Products with Digital Elements (Chap. III)

- **Presumption of conformity (18)**
  - Presumption of conformity with Annex I essential requirements when products and processes meet EU published harmonised standards
- **Common specifications (19)**
  - EC has power, subject to certain requirements, to establish common specifications to cover technical requirements and a means to comply with Annex I requirements
  - EC shall assess harmonised standards adopted by ESO to meet Annex I requirements
- **EU declaration of conformity (20)**
  - EU declaration of conformity shall be drawn up by manufacturers in accordance with Article 10(7) and state that the fulfilment of the applicable essential requirements set out in Annex I has been demonstrated
  - By drawing up the EU declaration of conformity, the manufacturer shall assume responsibility for the compliance of the product
- **General principles of CE marking (21)**
  - Subject to Regulation (EC) No 765/2008
- **Rules and conditions for affixing the CE marking (22)**
  - 7 requirements, including identifier of the conformity assessment body when required
- **Technical documentation (23)**
  - 5 extensive requirements for manufacturer technical documentation, including 12 Annex V requirements
- **Conformity assessment procedures for products with digital elements (24)**
  - Product manufacturers shall perform a conformity assessment of the product with digital elements and the processes put in place by the manufacturer to determine whether the essential requirements set out in Annex I are met
  - Product manufacturer or the manufacturer's authorised representative shall demonstrate conformity with the essential requirements by using one of the Annex VI modules
  - Manufacturers of Class 1 critical products shall follow certain procedures shall undertake conformity assessment with the essential requirements using one of the Annex VI modules
  - European Health Regulation systems shall demonstrate conformity under EHR rules
- **Mutual recognition agreements (24a)**
  - EC shall endeavour to conclude MRAs with third countries that are on a comparable level of technical development, have a compatible approach concerning conformity assessment, and ensure the same level of protection as the CRA provides

Notification of Conformity Assessment Bodies (Chap. IV)

- **Notification (25)**
  - Member States shall notify the Commission and the other Member States of conformity assessment bodies authorised to carry out CRA conformity assessments
- **Notifying authorities (26)**
  - Member States shall designate a notifying authority responsible for assessment, notification, and monitoring of conformity assessment bodies
- **Requirements relating to notifying authorities (27)**
  - 7 requirements specified
- **Information obligation on notifying authorities (28)**
  - Member States shall inform the EC of their procedures
- **Requirements relating to notified bodies (29)**
  - 23 requirements specified
- **Presumption of conformity of notified bodies (30)**
  - Must demonstrate its conformity with harmonised standards
- **Subsidiaries of and subcontracting by notified bodies (31)**
  - Must ensure subcontractors are in conformance
- **Application for notification (32)**
  - Specifies information required by conformity assessment body
- **Notification procedure (33)**
  - Notifying authority shall notify the EC and other Member States about their conformity assessment bodies
- **Identification numbers and lists of notified bodies (34)**
  - EC will assign identification number for a notified body and list
- **Changes to notifications (35)**
  - Notifying authority may restrict, suspend or withdraw notification
- **Challenge of the competence of notified bodies (36)**
  - EC may investigate competence of notified body and de-certify
- **Operational obligations of notified bodies (37)**
  - Notified bodies shall carry out conformity assessments as specified, and can require manufacturers take corrective actions, and decertify for non-compliance
- **Information obligation on notified bodies (38)**
  - Notified bodies must inform notifying authority of its compliance actions
- **Exchange of experience (39)**
  - EC shall provide for exchange of experience among national authorities responsible for notification policy
- **Coordination of notified bodies (40)**
  - EC shall ensure coordination and cooperation among notified bodies

Market Surveillance and Enforcement (Chap. V)

- **Market surveillance and control of products with digital elements in the Union market (41)**
  - Each Member State shall designate one or more market surveillance authorities for the purpose of ensuring the effective implementation and cooperate with certification authorities and designated CSIRTS, ENISA , EC and other market surveillance authorities; and consult with CRA Expert Group and ADCO
- **Access to data and documentation (42)**
  - Compels access to the data required to assess the design, development, production and vulnerability handling of such products, including related internal documentation
- **Procedure at national level for products with a significant cybersecurity risk (43)**
  - 13 required actions
- **Union safeguard procedure (44)**
  - 5 procedures for conflicts on actions among Member States
- **Procedure at EU level for products with a significant cybersecurity risk (45)**
  - 7 required actions
- **Compliant products with digital elements which present a significant cybersecurity risk (46)**
  - Authorities may compel all appropriate measures to ensure that the product with digital elements and the processes put in place by the manufacturer concerned, when placed on the market, no longer present that risk, to withdraw the product with digital elements from the market or to recall it within a reasonable period
- **Formal non-compliance (47)**
  - Authority can make non-compliance finding and compel manufacturer to end non-compliance and the Member State shall take all appropriate measures to restrict or prohibit the product with digital elements from being made available on the market or ensure that it is recalled or withdrawn from the market
- **Joint activities of market surveillance authorities (48)**
  - Authorities shall carry out joint activities for products placed or made available on the market, including those proposed by the EC and ENISA based on indications or information of potential non-compliance, and may use any information resulting from the activities carried out as part of any investigation that it undertakes
- **Sweeps (49)**
  - Authorities shall regularly conduct simultaneous coordinated control actions (“sweeps”) of particular products with digital elements or categories thereof to check compliance with or to detect infringements to this Regulation, including under a cover identity, to verify the compliance

Delegated powers and procedure (Chap. VI)

- **Exercise of EC delegation of power (50)**
  - Art. 2(4) Amend Annex I requirements limits and exclusions
  - Art. 6(2) Amend Annex III enumerated product sectors
  - Art. 6(3) Supplement Annex III enumerated product sector definitions
  - Art. 6(5) Specify categories of highly critical products requiring a European cybersecurity certificate at a “high” assurance level ‘high’
  - Art. 10(15) Specify the format and elements of the software bill of materials in Annex I
  - Art. 11(5) Specify the format and procedure of the notifications submitted by manufacturers for actively exploited vulnerabilities and incidents impacting security of a product
  - Art. 18(4) Specify European cybersecurity certification schemes used to demonstrate conformity of products with digital elements with Annex I essential requirements or parts thereof as set out in Annex I and issuance of a cybersecurity certificate at assurance level ‘substantial’ or ‘high’ that eliminates the obligation of a manufacturer to carry out a third-party conformity assessment
  - Art. 19(1) Establishing common specifications that cover technical requirements providing a means to comply with the requirements set out in Annex I for products where certain conditions have been fulfilled
  - Art. 20(5) Adding elements to the minimum content of the EU declaration of conformity set out in Annex IV to take account of technological developments
  - Art. 23(5) Adding elements to be included in the technical documentation set out in Annex V to take account of technological developments, as well as developments encountered in the implementation process of this Regulation
- **EC Committee procedure (51)**
  - The Commission shall be assisted by a committee following certain procedures

Confidentiality and penalties (Chap. VII)

- **Confidentiality (52)**
  - All parties subject to the CRA provisions are required to respect the confidentiality of the significant information emerging from implementation and criminal penalties may be imposed
- **Penalties (53)**
  - Member States are required to penalize infringements by economic operators, taking into account financial resources of microenterprises and small and medium-sized enterprises
  - Non-compliance of
    - Annex I requirements may result in fines of € 15 million or 2.5 % of annual global revenue
    - Any other requirements may result in fines of € 10 million or 2 % of annual global revenue
  - Supply of incorrect, incomplete or misleading information to notified bodies and market surveillance authorities may result in fines of € 5 million or 1 % of annual global revenue
  - Penalty information by be shared among Member States
  - Administrative fines may be imposed on public authorities
  - Market surveillance authorities may impose any other corrective or restrictive measures
- **Allocation of the revenue from penalties (53a)**
  - Member States shall allocate fine revenue to cybersecurity projects, including increasing skilled professionals, capacity building for smaller enterprises, and tools to prevent intellectual property theft

The next five slides summarize the 20 Jul 2023 draft European Commission request to the European Standardisation Organisations to produce “harmonised standards” to implement the CRA

CRA harmonised standards implementation and requirements

- **EC Implementing Decision to ESOs for CRA harmonised standards**
- **Draft by 31 May 2025 new or revise existing European standards or European standardisation deliverables, as listed in [CRA Annex III], and meet the "Requirements for the European standards and European standardisation deliverables"**
- **Presumption of conformity given by harmonised standards or parts thereof is particularly relevant for the *critical products with digital elements* listed in Annex III**
  - Class I products benefit from harmonised standards because they could remove the obligation to carry out third-party conformity assessment
  - Class II products benefit from harmonised standards because they support the development of conformity assessment activities and support market players in ensuring compliance of their products
- **Modes of cooperation between the ESOs and other international standardisation organisations may be established to benefit from possible synergies with existing international standards**
- **The EC Joint Research Centre together with ENISA have mapped existing international and European standards to initiate a discussion and carry out a detailed gap analysis**
- **Necessitates preparation of a work programme for submission to the EC**
- **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, and indicate clearly the correspondence between technical specifications and the essential cybersecurity requirements they aim to cover**
- **The policy objectives of the Commission in adopting the proposed Cyber Resilience Act should be taken into account when drafting deliverables in reply to this request, they are consistent with the EU legal framework, and consider any other relevant on-going European standardisation work related to other Union legislation**

Requirements for the European standards and European standardisation deliverables - all

- **Deliverables shall reflect the generally acknowledged state of the art 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**
- **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 verification, validation and testing procedures, objectively verifiable criteria and implementable methods to assess compliance with such specifications**
- **Deliverables shall clearly indicate its scope, the products which fall under its scope, and which risks are covered (if applicable)**
  - Where a 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 deliverable does not mitigate major risks identified after an exhaustive 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
- **Specifications that are relevant for conformity assessment activities, whether by the manufacturer in self-assessment or by a third-party, shall take into account the four CRA Annex VI modules**
- **Draft programme is due to the EC 2 months after notification**
- **Reporting to the EC will occur every 6 months with a final report in 2026**

Requirements for the European standards and European standardisation deliverables - specific

- **Product-agnostic cybersecurity requirements relating to the properties of products with digital elements (3 requirements)**
  - Deliverables should take into account the interdependencies between the different requirements reflected in the standards, especially for CRA Annex III Class 1 products, and to the extent possible reflect them explicitly in the corresponding specifications
- **Vulnerability handling requirements for *products with digital elements* (9 requirements)**
  - Deliverables 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
- ***Product-specific cybersecurity requirements relating to the properties of products with digital elements***
  - Deliverables shall provide specifications for the cybersecurity requirements of specific products or, when appropriate, product categories, especially for CRA Annex III Class 2 products, and treat links to NIS2 areas
  - Deliverable shall be drafted to ensure that the harmonised standards to follow after the entry into force of the CRA provide presumption of conformity regarding the sets of risks they identify, and adequately cover all major risks identified after an exhaustive analysis

Requested standards deliverables - 1

Essential cybersecurity requirements for *products with digital elements*

Request #

1. Delivering products with digital elements without known exploitable vulnerabilities *
2. Delivering products with digital elements with a secure by default configuration, unless otherwise agreed between the parties in a business-to-business context, including the possibility to reset the product to its original state while retaining all installed security updates *

2a. Delivering products where technically feasible, be made available on the market with functional separation of security updates from functionality update *

2b. Delivering products that ensure automatic security updates with a clear and easy-to-use opt-out mechanism and the notification of available updates to users*

3. Ensuring protection of products with digital elements from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems
4. Protecting the confidentiality of data, personal or other, stored, transmitted or otherwise processed by a product with digital elements, such as by encrypting relevant data at rest or in transit by state of the art mechanisms, and by using other technical means *
5. Protecting the integrity of personal or other 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 or possible unauthorised access *
6. Processing only personal or other data that are adequate, relevant and limited to what is necessary in relation to the intended use of the product with digital elements ('minimisation of data')
7. Protecting the availability of essential and basic functions, also after an incident, including with backup management, and the resilience and mitigation measures against denial of service attacks *
8. Minimising the negative impact of a product with digital elements on the availability of services provided by other devices or networks
9. Designing, developing and producing products with digital elements with limitted attack surfaces, including external interfaces
10. Designing, developing and producing products with digital elements that reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques
11. Providing provide security related information by recording and/or monitoring capabilities for relevant internal activity, including the access to or modification of data, services or functions, with an opt-out mechanism for the user *

~~12. Ensuring that vulnerabilities in products with digital elements can be addressed through security updates, including, where applicable, through automatic updates and the notification of available updates to users~~ *

11a. Enabling users to securely withdraw and remove their data on a permanent basis. *

13. Vulnerability handling for products with digital elements [as specified in Annex I, 2] **

* Added or amended in new CRA revision

Requested standards deliverables - 2

Essential cybersecurity requirements for *critical products with digital elements in Annex III*

Request #

14. Identity management systems software and privileged access management software
15. Standalone and embedded browsers
16. Password managers
16a. Biometric readers*
17. Software that searches for, removes, or quarantines malicious software
18. Products with digital elements with the function of virtual private network (VPN)
19. Network management systems
20. Network configuration management tools
21. Network traffic monitoring systems
22. Management of network resources
23. Security information and event management (SIEM) systems
24. Update/patch management, including boot managers*
25. Application configuration management systems
26. Remote access software*
27. Mobile device management software
28. physical and virtual network interfaces*
29. operating systems not covered by Class II*
30. Firewalls, intrusion detection and/or prevention systems not covered by Class II*
31. Routers, modems intended for the connection to the internet, and switches, including specifically those intended for industrial use
32. General purpose microprocessors and microprocessors not covered by Class II*
33. Microcontrollers
34. Application specific integrated circuits (ASIC) and field-programmable gate arrays (FPGA) intended for the use by essential entities of the type referred to in Article 3 of Directive(EU) 2022/2555;
35. Industrial Automation & Control Systems (IACS) not covered by class II, such as programmable logic controllers (PLC), distributed control systems (DCS), computerised numeric controllers for machine tools (CNC), industrial robots and their control systems and supervisory control and data acquisition systems (SCADA)
36. Industrial internet of things not covered by Class II*

36a. Home automation systems, including smart home servers and virtual assistants*
36b. Security devices, including smart door locks, cameras and alarm systems*
36c. Smart toys*
36d. Personal health appliances and wearables*
36e. Operating systems for servers, desktops, and mobile devices**
37. Hypervisors and container runtime systems that support virtualised execution of operating systems and similar environments
38. Public key infrastructure and digital certificate issuers
38a. firewalls, intrusion detection and/or prevention systems intended for industrial use**
- ~~general purpose microprocessors~~ *
38b. Microprocessors intended for integration in programmable logic controllers and secure elements**
38c. Routers, modems intended for the connection to the internet, and switches*
39. Secure elements
40. Hardware Security Modules (HSMs)
41. Secure cryptoprocessors
42. Smartcards, smartcard readers and tokens
42a. Industrial Automation & Control Systems (IACS) intended for the use by essential entities of the type referred to in Article 3 of Directive (EU) 2022/2555, such as programmable logic controllers (PLC), distributed control systems (DCS), computerised numeric controllers for machine tools (CNC) and supervisory control and data acquisition systems (SCADA) **
42b. Industrial Internet of Things devices, including specifically those intended for use by essential entities of the type referred to in Annex I to Directive (EU) 2022/2555) **
~~43. Robot sensing and actuator components and robot controllers~~ *
44. Smart meters

Key: black=Class I products; blue=Class II products

* Added or amended in new CRA revision
** Omitted in EC request

Collected public and analyst assessments

CRA implementation impediments & challenges

- **Scale and complexity of implementation requirements**
  - Inability to apply requirements to all market products with digital elements and remote processing solutions and obligations to economic operators worldwide
  - Inability for economic operators and CRA institutions to know or implement what is required
  - Inability to develop implementable standards and guides
- **Technical, operational, economic, and institutional inabilities to achieve**
  - Some requirements are not achievable or reasonable
  - Market availability is not controllable
  - Enormous resources and costs are required to pursue
  - Lack of meaningful benefit compared to NIS2 requirements
  - Lack of compatibility with existing cybersecurity ecosystems
  - Collateral adverse cybersecurity effects; hacking CRA information
  - Inability to harmonise across dozens of diverse EU legal instruments
  - Paywall standards
- **Opposition of national jurisdictions and economic operators**
  - Conflicting national cybersecurity and regulatory strategies
  - Opposition to asserting extraterritorial jurisdiction and Conflict of Law
  - Rights abuses against economic operators
  - Enforceability – unreasonable requirements and excessive penalties result in juridical challenges
  - Draconian compliance surveillance resources more effectively spent on defense controls
  - Many cybersecurity standards already exist in other international standards organizations
  - Extreme vagueness and complexity will lead to arbitrary and capricious enforcement
  - CRA institutional complexity prevents necessary levels of confidentiality
  - Explicit national CRA bounty hunting policies may lead to unlawful entrapment
  - National jurisdictions including EU Members together with economic operators and individuals worldwide will not support
  - Significant decrease in cybersecurity for European citizens
  - Significant adverse EU economic harm for competitiveness, product and service unavailability, and competition distortions