ISSN 1831-9424

European Commission

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

Cyber Resilience Act Requirements Standards Mapping

Joint Research Centre & ENISA Joint Analysis

EUR 31892 EN

JRC137340
EUR 31892 EN
PDF ISBN 978-92-68-14180-9 ISSN 1831-9424 doi:10.2760/905934 KJ-NA-31-892-EN-N
Luxembourg: Publications Office of the European Union, 2024

How to cite this report: Hernandez Ramos, J.L., Karopoulos, G., Nai Fovino, I., Spigolon, R., Sportiello L., Steri, G., Gorniak, S., Magnabosco, P., Atoui, R., Crippa Martinez, C., *Cyber Resilence Act Requirements Standards Mapping*, Publication Office of the European Union, 2024, https://data.europa.eu/doi/10.2760/905934, JRC137340.

About JRC

The Joint Research Centre is the European Commission's science and knowledge service. The JRC is a Directorate-General of the European Commission under the responsibility of the Commissioner for Innovation, Research, Culture, Education and Youth. Our researchers provide EU and national authorities with solid facts and independent support to help tackle the big challenges facing our societies today. Our headquarters are in Brussels and we have research sites in five Member States: Geel (Belgium), Ispra (Italy), Karlsruhe (Germany), Petten (the Netherlands) and Seville (Spain). Our work is largely funded by the EU's budget for Research and Innovation. We create, manage and make sense of knowledge, delivering the best scientific evidence and innovative tools for the policies that matter to citizens, businesses and governments. For more information, visit https://ec.europa.eu/jrc.

About ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. For more information, visit www.enisa.europa.eu .

Contact information

For contacting the authors, please use https://ec.europa.eu/jrc/en/contact/form or resilience@enisa.europa.eu

Authors

JRC
Hernandez Ramos, J.
Karopoulos, G.
Nai Fovino, I.
Spigolon R.
Sportiello L.
Steri, G.

ENISA
Gorniak, S.
Magnabosco, P.

Atoui, R.
Crippa Martinez, C.

Acknowledgements

The authors would like to thank colleagues of DG CNECT.H2 for their review of this report.

Contents

Abstract

The increasing number of cyberattacks affecting digital products, coupled with widespread vulnerabilities and insufficient timely security updates, creates heavy financial burdens on society. In response, the European Commission has drafted the Cyber Resilience Act (CRA), a new proposal for regulation to define the legislative framework of essential cybersecurity requirements that manufacturers must meet when placing any product with digital elements on the internal market.

To facilitate adoption of the CRA provisions, these requirements need to be translated into the form of harmonised standards, with which manufacturers can comply. In support of the standardisation effort, this study attempt to identify the most relevant existing cybersecurity standards for each CRA requirement, analyses the coverage already offered on the intended scope of the requirement and highlights possible gaps to be addressed.

1 Introduction

On 15 September 2022, the European Commission published the proposal for the *Cyber Resilience Act (CRA)* [1], a proposal for a first ever EU-wide legislation of its kind, aimed at introducing mandatory cybersecurity requirements for products with digital elements throughout their lifecycle.

The CRA proposal covers all products with digital elements put on the market which can be connected to a device or a network, including their building blocks (i.e., hardware and software) and encompassing also solutions provided in a Software as a Service (SaaS) fashion if they qualify as remote data processing solutions, as defined by Article 3(2) of the CRA proposal.

The CRA proposal provides two sets of essential requirements:

— *Product cybersecurity requirements* in Annex I, Section 1 of the CRA proposal

— *Vulnerability handling process requirements* in Annex I, Section 2 of the CRA proposal

These requirements should be the subject of a standardisation process by the European Standardisation Organizations (ESOs) to express them in the form of specifications in harmonised standards.

The general principle is that for the products on the market, a self-assessment of compliance with the requirements specified in Annex I will be sufficient. For certain categories of more critical products, the application of harmonised standards will be required. For even more critical products, a third-party assessment will be mandatory.

This report details the available standardisation outputs on the cybersecurity of products (hardware and software products, including hardware and software components of more complex products) carried out mainly by ESOs and international Standards Development Organizations (SDOs). Specifically, the study aim at presenting a mapping of the existing cybersecurity standards against the essential requirements listed in Annex I of the CRA proposal, along with a gap analysis between the mapped standards and the requirements. In view of the development of harmonised standards, this analysis offers a possible overview about the current coverage of the requirements by existing specifications, highlighting possible lacks that may be compensated by further standardisation work.

Upon request of DG CNECT, this study has been developed jointly by the Joint Research Centre (JRC) and the European Union Agency for Cybersecurity (ENISA). This was also in line with the expectations of the proposal of regulation, in which it is stated that synergies on standardisation aspects should be considered between the Commission and ENISA.

In Section 2, the methodology adopted to carry out this study is summarised. Section 3 is devoted to the presentation of the mapping between requirements and standards, giving an analysis of the coverage offered by the standards and possible gaps. In Section 4, a summary of all identified standards and their respective mapping is offered along with some overall remarks, while Section 5 is for conclusions.

2 Methodology

The development of the present study has been articulated in several stages summarised here below.

Identification of the standardisation organisations

The first step consisted in the identification of the entities that are considered relevant for standards in the specific area and that are recognised by the industry and scientific communities, giving precedence to European and international standardisation organisations. Specifically, the following ones have been taken into account:

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

Identification of the committees and related standardisation activities

For each of the organisations listed above, the respective committees working on cybersecurity standards have been identified. For each one of the identified committees the list of standardisation activities, including ongoing activities, with potential relevance for the mapping have been identified, drafting a list of respective standards.

High level analysis of the standardisation activities

The standards identified above have been analysed based on freely available information to confirm their relevance to the specific topic. For those considered relevant a tentative mapping to the cybersecurity requirements expressed in Annex I of the CRA Regulation has been proposed, while the others have been discarded. Some statistics pertaining to this activity are summarised in Annex I of the present document, so as to give an order of magnitude of its extent. This high-level overview represented a preparatory ground for the insightful analysis of the next stage.

Mapping and analysis of requirements against standards

Once we listed all standards that might be relevant in a first quantitative analysis, the analysis took a bottom-up approach. For each CRA requirement the most relevant standards were selected based on an expert analysis, allowing to identify both the currently offered coverage and the potential gaps to be addressed at later standardisation stages. The requirements mapping and analysis process is presented in Figure 1, and the overall output of this stage is presented in Section 3.

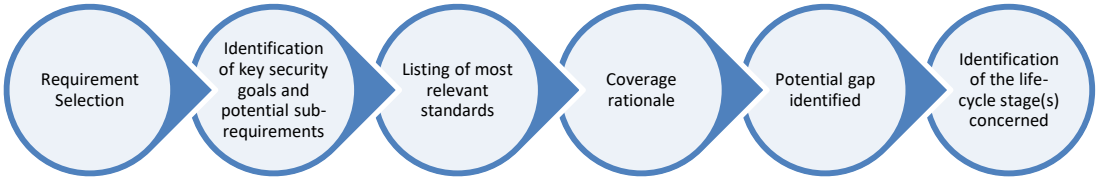

Figure 1 Overall requirements mapping and analysis process

The CRA cybersecurity essential requirements are presented in a list, and each of them is expressed in the form of generic text. To enhance the identification and evaluation of the standards possibly covering aspects captured by the CRA requirements it has been deemed useful to analyse them and highlight some core concepts. Specifically, for each essential requirement a set of sample sub-requirements and keywords have been identified. Such elements have served mainly as guide to identify the CRA-relevant standards, but there are not intended to represent a comprehensive list of sub-requirements, as a specific break-down of a requirement may depend on specificities of products and applications. To be noted that when an identified standard was available both in the form of international standard and European standard, we have referenced it according to the latter.

In addition to the requirements-standards mapping, since the security requirements may apply to different stages of the products life-cycle, the study have been enriched with an information pointing out the possible relevance of a requirement with specific product life-cycle stages. This may be helpful under a manufacturer point of view to better navigate through the requirements and standards depending on at what stage a product is. The following high-level generic life-cycle that applies to all diversity of products has been taken as reference.

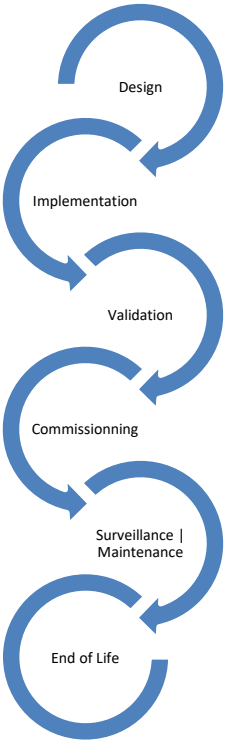

Figure 2 Generic product life-cycle

3 Requirements-Standards mapping and analysis

Here below each CRA requirement is mapped against relevant standards. For each standard is discussed the level of coverage offered for the requirement and possible gaps to be considered. For each requirement all the analysis are summarized in an overall consideration. The two sub-sections below reflect the two groups of requirements expressed in the CRA Annex I.

3.1 Security requirements relating to the properties of products with digital elements

3.1.1 (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;

Sample Sub-requirements:

— A cybersecurity risk analysis should be conducted and monitored during the complete lifecycle of the product

— Cybersecurity should be taken into account in every step of the product creation (e.g. secure coding, security by design principles, etc.)

Keywords: risk, risk analysis, remediation strategy, secure coding

Standard ID	Standard title	Rationale	Gap	Life-Cycle
EN ISO/IEC 27002: 2022	Information security, cybersecurity and privacy protection — Information security controls	ISO 27002 includes controls related to secure coding and information security in supplier agreements (demanding that the suppliers ensure its products/components have the required level of security, and communicate all information regarding external software and components used)	While there are indications for software development like the secure coding part, analogous indications for a secure hardware design are missing in this standard, although a more generic “Secure system architecture and engineering principles” could in principle make up for it in all those cases where hardware is acquired and incorporated but not designed.	Implementation Validation Commissioning Surveillance Maintenance

EN ISO/IEC 27005: 2022	Information security, cybersecurity and privacy protection — Guidance on managing information security risks	Although not specific to product security, this standard specifies how information security risks should be managed. A proper risk analysis is indeed of paramount importance to understand which is the "appropriate level of cybersecurity based on the risks"	This standard is generic and not specific to product development	Design
EN IEC 62443-3-2:2020	Security for industrial automation and control systems – Part 3-2: Security risk assessment for system design	Although specific only to Industrial Automation and Control Systems (IACS), this standard covers in detail a Security Risk Assessment process focused on a system design, including the re-evaluation phase after proper countermeasures have been implemented, determining the presence of residual and tolerable risks	This standard applies only to Industrial Automation and Control System and does not cover cybersecurity principles like security by design	Design Implementation Validation
EN IEC 62443-4-1:2018	Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements	Although specific only to Industrial Automation and Control Systems (IACS), this standard prescribes security principles (i.e. security by design) to be included during the various phases of a product development.	This standard applies only to Industrial Automation and Control System and does not cover the concept of risk assessment	Design Implementation Validation
ETSI EN 303 645	CYBER; Cyber Security for Consumer	Promotes secure development and maintenance	Detailed guidelines on risk analysis and secure practices are	Design Maintenance

V2.1.1 (2020-06)	Internet of Things: Baseline Requirements	practices, implies the need for risk analysis by setting a framework for secure design, emphasizes secure development practices and data protection	not provided, but sometimes references to relevant documents are provided.	
Overall coverage and possible gaps	The various components of this requirement are covered within major cybersecurity standards. Within these three selected standards, the gaps may be summarised as follow: — The hardware design part is less covered when compared to the software counterpart — A risk analysis process specifically targeted to system design is presented only for IACS, while the more general ISO 27005 standard is not specific to system or product design			

Table 1: Mapping of security requirement No. 1

3.1.2 (2) Products with digital elements shall be delivered without any known exploitable vulnerabilities;

Sample Sub-requirements:

— A vulnerability assessment should be performed against the digital elements of a product

— Known exploitable vulnerabilities shall be fixed before the release of the product

Keywords: exploitable vulnerability, vulnerability assessment

Standard ID	Standard	Rationale	Gap	Life-Cycle
ISO/IEC 18045: 2022	Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Methodology for IT security evaluation (note: this is the standard used for the Common Evaluation	Describes the minimum actions to be performed for a generic IT security evaluation. It includes a dedicated section on vulnerability assessment. This section describes the main elements that should be present in a vulnerability assessment with specific steps and activities to be followed (such as penetration testing). (note: it is intended to be used in conjunction with the	Covers only vulnerability discovery and not fixing vulnerabilities. Cites only one discovery technique (penetration testing).	Validation

	Methodology (CEM))	Common Criteria - ISO/IEC 15408 series)		
ITU-T X.1214 (03/2018)	Security assessment techniques in telecommunication/information and communication technology networks	Covers vulnerability detection of ICT network elements; both known and unknown (zero-day) vulnerabilities; covers different techniques: scanning, fuzzing, code review, binary analysis, penetration testing, plus some other supplementary techniques	Covers (software-based) ICT network elements. Vulnerability detection only, not fixing. There is no detailed step-by-step procedure but an example model that could be followed; the standard contains mainly a list of techniques that could be used, providing general descriptions of these techniques	Validation Surveillance Maintenance
EN IEC 62443-4-1:2018	Security for industial automation and control systems – Part 4-1: Secure product development lifecycle requirements	Although specific only to Industrial Automation and Control Systems (IACS), this standard contains several provisions related to security testing, like vulnerability testing and penetration testing. Moreover, it describes what this tests should cover, who should perform them, and how to manage identified cybersecurity issues	This standard applies only to Industrial Automation and Control System	Validation Surveillance Maintenance
ETSI EN 303 645 V2.1.1 (2020-06)	CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements	Provision 5.2-3 of the standard refers to secure development lifecycle including vulnerability management. Manufacturers should continually monitor for identifying and rectifying security vulnerabilities	The standard lacks explicit provisions regarding conducting a vulnerability assessment. There is no explicit	Validation

		within products and services they sell, produce, have produced and services they operate during the defined support period.	requirement to fix each known exploitable vulnerability before the release of the product	
Overall coverage and possible gaps	The first two standards (ISO/IEC 18045:2022 and ITU-T X.1214) contain a step-by-step methodology for vulnerability assessment; collectively they cover the pre- and post-delivery phases of the product life cycle. They cover both known and unknown (zero-day) vulnerabilities with a number of different, complementary techniques. The IEC 62443-4-1 standard prescribes several security tests on the product, although referring only IACS, and the ETSI EN 303 645 standard poses a requirement for IoT manufacturers not referring explicitly to the initial delivery and without further implementation detail. With the exception of the IEC 62443-4-1 standard, but which refers only to IACS, the main identified gap is that the mentioned standards cover only vulnerability detection and not the patching of the discovered vulnerabilities, so in general not covering the whole requirement: ISO/IEC 18045 (which is the standard used for the Common Evaluation Methodology (CEM) that is used in conjunction with the Common Criteria - ISO/IEC 15408 series) describes a vulnerability assessment methodology in validation phase and with only one technique, ITU-T X.1214 covers more techniques in validation and maintenance phases but without a specific methodology and focusing on ICT network elements, and ETSI EN 303 645 describes only the necessity to deliver products without vulnerabilities.			

Table 2: Mapping of security requirement No. 2

3.1.3 (3) On the basis of the risk assessment referred to in Article 10(2) and where applicable, products with digital elements shall:

(a) be delivered with a secure by default configuration, including the possibility to reset the product to its original state;

Sample Sub-requirements:

- In case default configurations foresee an initial/default credential, the same should use a complex and randomly chosen password, different for each product
- In case default configurations cover cybersecurity items, they should adopt a reasonable level of security for each item
- The default configuration should be placed in a non-erasable memory
- A function to reset the product configuration to the default one should be implemented

Keywords: default configuration, randomised password, unique password, non-erasable memory, ROM, reset, security by default

Standard ID	Standard title	Rationale	Gap	Life-Cycle
EN ISO/IEC 27002: 2022	Information security, cybersecurity and privacy protection — Information security controls	This standard provides a set of generic controls for information security risk treatment. It includes implementation guidance for the controls based on recognised best practices. Among the technological controls there is configuration management, which addresses security configuration of hardware, software, services and networks.	It mainly provides general guidelines covering several different aspects, so it does not specifically target this requirement.	Implementation Validation
ETSI EN 303 645 V2.1.1 (2020-06)	CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements	This standard defines cybersecurity provisions for consumer IoT devices. Among those there are recommendations on the use of default passwords on the devices, secure storage of sensitive parameters and the management of the credentials (e.g., password generation, user authentication and change of default values)	The provisions are expressed at high-level without details for a reasonable security level in the default configuration and target specifically consumer IoT devices.	Design Implementation
ISO/IEC 18031: 2011	Information technology — Security techniques — Random bit generation	This standard defines the conceptual model of non-deterministic and deterministic random bit generators for	The standard is dedicated to the definition of models for random bit generation, thus not specifically	Design Implementation

		cryptographic purposes. It specifies their security requirements and covers application of random bit strings for random PIN and password generation. It can be employed to address aspects of randomised passwords and keys for secure product configuration.	targeting configuration management aspects.	
Overall coverage and possible gaps	Aspects related to random password and key generation in general are well covered by ISO/IEC 18031:2011 for what concerns specific conceptual models. Those related to product configuration/credentials management (ISO/IEC 27002:2022 and ETSI EN 303 645) are addressed at a high level, with references to NIST publications for details. More detailed implementation aspects relying for example on the specific use of non-erasable memories for configuration management seem not to be covered.			

Table 3: Mapping of security requirement No. 3a

3.1.4 (3b) ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems;

Sample Sub-requirements:

— In accordance with the nature of the product and to the relevant risks identified in the risk analysis, an appropriate system to provide authentication and authorisation should be implemented.

— The access to personal/protected data and to administration/configuration functions should be granted only to authenticated and authorised users

— In accordance with the nature of the product and to the relevant risks identified in the risk analysis, physical unauthorized access should be forbidden

Keywords: authentication, authorisation, identity & access management, IAM, physical access control, logical access control, anti-tampering

Standard ID	Standard	Rationale	Gap	Life-Cycle
ISO/IEC 9798 **Parts 1 to 6**	Information technology — Security techniques — Entity authentication — Part 1:2010 General Part 2:2019 Mechanisms using authenticated encryption Part 3:2019 Mechanisms using digital signature techniques Part 4:1999 Mechanisms using a cryptographic check function Part 5:2009 Mechanisms using zero-knowledge techniques Part 6:2010 Mechanisms using manual data transfer	The General part of the ISO/IEC 9798 standard specifies a model for entity authentication, together with general requirements and constraints for the relevant mechanisms. It covers a variety of authentication protocols, including one-to-one and through a third-party authentication. Details for specific mechanisms are provided in the other Parts of this standard.	Covers only authentication.	Design Implementation
ISO/IEC 24760 **Parts 1 to 3**	IT Security and Privacy — A framework for identity management Part 1:2019 Terminology and concepts Part 2:2015 Reference architecture and requirements Part 3:2016 Practice	This series of standards specifies a framework for issuing, administering, and managing identity data and applies to any information system. Part 1 defines terms and core concepts of identity and identity management. Part 2 provides guidelines and	Covers only identity management systems; does not cover access management.	Design Implementation Validation

		requirements for the implementation of an identity management framework. Part 3 provides guidance for ensuring that an identity management system conforms to Parts 1 and 2.		
ISO/IEC 29146: 2016	Information technology — Security techniques — A framework for access management	This standard defines a framework for access management, building on top of an identity management system (not covered in this standard). It describes the process to access ICT resources in a secure and accountable way.	Covers access management only; does not cover identity management which is a pre-requisite for this framework.	Design
ITU-T X.1253 (09/2011)	Security guidelines for identity management systems	This standard provides guidelines for the secure and privacy-preserving deployment and operation of identity management systems.	It is of generic nature and does not apply to specific identity management systems; as such, high-level descriptions of the techniques are provided.	Design
ITU-T X.812 (11/1995)	Information technology – Open Systems Interconnection – Security frameworks for open systems: Access control framework	Provides a general overview of access control, policies and mechanisms. It can be used by standards describing	It is generic and does not describe specific access control mechanisms or steps to be performed to	Design

		specific access control mechanisms and services.	provide access control services.	
ETSI EN 303 645 V2.1.1 (2020-06)	CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements	Provisions 5.1, 5.5: require authentication, unique passwords, and cryptographic measures.	The standard emphasizes authentication and cryptography, but lacks specifics on access management systems.	Design Implementation
EN IEC 62443-4-2:2019	Security for industial automation and control systems – Part 4-2: Technical security requirements for IACS components	This standard, related to IACS components, includes requirements that cover the various aspects of user authentication (all provisions included in Foundational Requirement 1 – Identification and authentication control) and authorisation (Component requirement 2-1: Authorisation enforcement)	This standard applies only to Industrial Automation and Control System	Design Implementation
Overall coverage and possible gaps	The standards above cover the following areas: authentication, identity & access management, and access control. The aspects related with these areas are well covered by the above standards. It should be noted that the above standards are mainly of generic nature and in most cases do not cover specific mechanisms and services.			

Table 4: Mapping of security requirement No. 3b

3.1.5 (3c) 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;

Sample Sub-requirements:

— Data stored in a product's internal memory should be encrypted at rest using current non-deprecated technology

— Transmission protocols used to send/receive data should support encrypted communications and enable them by default

— The product should implement symmetric or asymmetric encryption schemes (including PKIs) to ensure that confidentiality of exchanged data is protected

Keywords: symmetric/asymmetric encryption, encryption at rest and in motion/transit, PKI, certificates, sensitive assets confidentiality, data confidentiality

Standard ID	Standard	Rationale	Gap	Life-Cycle
ITU-T X.805 (10/2003)	Security architecture for systems providing end-to-end communications	This standard describes a generic architecture for end-to-end communication security that is independent of the network technology or protocol stack layer.	Does not cover protection of data at rest; very generic, covers the basic principles that should be followed by security mechanisms without describing specific mechanisms.	Design
ISO/IEC 18033 **Parts 1 to 7**	Information security — Encryption algorithms — Part 1:2021 General Part 2:2006 Asymmetric ciphers Part 3:2010 Block ciphers Part 4:2011 Stream ciphers Part 5:2015 Identity-based ciphers	This series of standards describes encryption algorithms for data confidentiality both for stored and transmitted data. It covers symmetric and asymmetric ciphers but also non-conventional algorithms such as homomorphic and	These standards do not describe key management; only an overview is given in Part 1 with relevant references. Some algorithms are deprecated	Design Implementation

	Part 6:2019 Homomorphic encryption Part 7:2022 Tweakable block ciphers	identity-based ciphers.		
ITU-T X.814 (11/1995)	Information technology – Open Systems Interconnection – Security frameworks for open systems: Confidentiality framework	This standard defines the basic concepts related to confidentiality, discussing also types of confidentiality services, mechanisms, threats and attacks.	It is very generic, covers the basic principles of confidentiality without describing specific protocol exchanges	Design
ETSI EN 303 645 V2.1.1 (2020-06)	CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements	Provisions 5.5.1, 5.5.6, 5.5.7 focus on secure communication and confidentiality using cryptography. Provisions 5.8.1, 5.8.2 ensure cryptographic protection of personal data. Provisions 5.4.1, 5.4.4 require secure storage and uniqueness of security parameters.	The standard lacks specific coverage for protecting all data types, in particular at rest, and does not fully address particular encryption schemes.	Design Implementation
EN IEC 62443-4-2:2019	Security for industial automation and control systems – Part 4-2: Technical security requirements for IACS components	This standard, related to IACS components, includes a confidentiality requirement for both data at rest and in transit (Component Requirement 4.1: Information Confidentiality)	This standard applies only to Industrial Automation and Control System. Moreover, the confidentiality requirement is quite generic and does not provide technical details	Design Implementation

Overall coverage and possible gaps	The above standards cover the basic concepts and principles behind data confidentiality, both at-rest and in-transit. They also cover symmetric and asymmetric encryption algorithms, as well as homomorphic and identity-based ciphers. The aspects related with these areas are well covered by the above standards. It should be noted here that the above standards are a mix of generic standards independent from network technology or network stack layer and more specific standards describing encryption algorithms.

Table 5: Mapping of security requirement No. 3c

3.1.6 (3d) protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, as well as report on corruptions;

Sample Sub-requirements:

- Integrity of data, programs and configurations stored in the product's internal memory should be ensured using current non-deprecated technology, e.g. hashing
- Transmission protocols used to send/receive data should support ways to ensure it is possible to spot data alteration during the transmission (e.g. MACs)
- The product should implement symmetric or asymmetric encryption schemes (including PKIs) to ensure that the integrity of exchanged data is protected
- A product should perform self-test to verify integrity of relevant code/information (e.g. firmware)

Keywords: integrity, hashing, checksum, data corruption, PKI, certificates, self-test

Standard ID	Standard	Rationale	Gap	Life-Cycle
ISO/IEC 9796 **Parts 2 and 3**	Information technology — Security techniques — Digital signature schemes giving message recovery Part 2:2010 Integer factorization based mechanisms Part 3:2006 Discrete logarithm based mechanisms	Covers digital signatures where part or the entire message can be recovered from the signature. It describes deterministic and randomized mechanisms, specifying also the key production method.	Does not cover digital signatures with appendix; also, does not cover techniques for key management and random number generation.	Design Implementation
ISO/IEC 9797 **Parts 1 to 3**	Information technology — Security techniques — Message	These standards cover several MAC algorithms based on block ciphers, dedicated or universal hash	Does not cover key management of block cipher mechanisms.	Design Implementation

	Authentication Codes (MACs) Part 1:2011 Mechanisms using a block cipher Part 2:2021 Mechanisms using a dedicated hash-function Part 3:2011 Mechanisms using a universal hash-function	functions. Part 1 covers 6 MAC algorithms based on block ciphers, generic enough to be applied to any security architecture, process or application.		
ISO/IEC 14888 **Parts 1 to 3**	Information technology — Security techniques — Digital signatures with appendix Part 1:2008 General Part 2:2008 Integer factorization based mechanisms Part 3:2018 Discrete logarithm based mechanisms	Covers digital signatures where the entire message is stored and/or transmitted together with the signature. It describes several mechanisms, including identity-based, and certificate-based schemes.	Does not cover digital signatures with message recovery; also, does not cover techniques for key and certificate management, and random number generation.	Design Implementation
ITU-T X.815 (11/1995)	Information technology – Open Systems Interconnection – Security frameworks for open systems: Integrity framework	This standard defines the basic concepts related to integrity, also discussing types of integrity services, policies, mechanisms, threats and attacks.	It is of generic nature; covers the basic principles of integrity without describing specific mechanisms	Design
ETSI EN 303 645 V2.1.1 (2020-06)	CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements	The standard emphasizes secure storage (5.4), and software integrity (5.7).	While the standard covers many aspects of data integrity, it	Design Implementation

		These directly align with the requirement's focus on ensuring integrity using non-deprecated technology like hashing and cryptographic schemes	does not explicitly detail information integrity.	
EN IEC 62443-4-2:2019	Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components	This standard, related to IACS components, includes specific integrity requirements that cover software, updates, configuration, communications, audit logs, etc.	This standard applies only to Industrial Automation and Control System. Moreover, the integrity requirements although quite specific, do not seem to have a general applicability in all situation (e.g. there is not an integrity requirement prescribing all memory to have integrity protection feature, but this might be due to the specific nature of IACS)	Design Implementation
Overall coverage and possible gaps	The above standards cover basic concepts and principles for providing integrity services. They also describe specific mechanisms for integrity based on digital signatures and MACs. The aspects related with these areas are well covered by the above standards. It should be noted here that the above standards are a mix of generic (related to integrity concepts) and more specific standards (related to integrity mechanisms).			

Table 6: Mapping of security requirement No. 3d

3.1.7 (3e) process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended use of the product ('minimisation of data');

Sample Sub-requirements:

— In general, refer to GDPR best practices, such as:

- it should not be asked to the user the provision of data that is not strictly necessary to the execution of the task or service requested
- data no longer needed should be deleted without delay

Keywords: privacy, GDPR, data minimisation, personal data, data retention

Standard ID	Standard title	Rationale	Gap	Life-Cycle
ISO/IEC 27701: 2019	Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines	This standard is an extension to ISO 27001 and 27002 regarding privacy information management. It includes requirements and controls for this specific topic and mapping with relevant standards and legislation, like the GDPR.	This standard, being an extension of the ISO/IEC 27001 and 27002 standards, refers to organisations rather than products. Nevertheless, it could be argued that an organisation implementing the controls included in this standard will do the same for its products	Design Implementation Validation Commissioning Surveillance Maintenance End of Life
ISO/IEC 29100: 2011	Information technology — Security techniques — Privacy framework	This standard provides a high-level framework for the protection of PII within ICT systems. Although it is quite high-level and does not include concrete requirements and controls, it contains explanatory sections on key privacy concepts, including data minimisation	No specific requirements or controls are present in this document	Design Implementation Validation Commissioning Surveillance Maintenance End of Life

ETSI TS 103 485 V1.1.1 (2020-08)	CYBER; Mechanisms for privacy assurance and verification	This Technical Specification document describes mechanism to enable assurance of privacy, using references to Common Criteria documents and to the GDPR	The documents does not list specific requirements or controls	Design Implementation Validation Commissioning Surveillance Maintenance End of Life
ETSI EN 303 645 V2.1.1 (2020-06)	CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements	The standard addresses data protection and minimization, with provisions ensuring secure data handling, transparent processing, and adhering to the principles of only processing necessary data (e.g., Sections 5.8 and 6). The standard emphasizes secure and responsible data management, aligning with GDPR principles, thereby addressing the requirement to a considerable extent.	While the standard outlines broad measures for data security and processing, it lacks specific guidance for data minimization practices such as the deletion of unnecessary data and prevention of forced registrations. It would also benefit from better reference to some explicit GDPR-specific best practices to be more effective.	Design Implementation
Overall coverage and possible gaps	This privacy requirements is very well covered especially in the ISO/IEC 27701 standard, that proposes a mapping between various standards and legislation, including the GDPR. The concept of data minimisation is well covered.			

Table 7: Mapping of security requirement No. 3e

3.1.8 (3f) protect the availability of essential functions, including the resilience against and mitigation of denial of service attacks;

Sample Sub-requirements:

— The product should be hardened against attacks, like for instance distributed denial of service attacks, by implementing, among other things, the following measures if appropriate:

- reverse proxies network segmentation
- load balancing
- rate limiting
- redundancy and high availability solutions
- backup sites
- disaster recovery plans
- minimize offered services

Keywords: availability, resiliency, secure outages, backup, denial of service, DoS, DDoS, protocol-based attacks, connection limit

Standard ID	Standard title	Rationale	Gap	Life-Cycle
EN ISO/IEC 27002: 2022	Information security, cybersecurity and privacy protection — Information security controls	This standard provides a set of generic controls for information security risk treatment. It includes implementation guidance for the controls based on recognised best practices. Among the organisational controls there is information transfer, which mentions denial of service protection for electronic messaging and availability of services and information	The guidance for developing availability of essential functions is provided at a high level (e.g., for DoS protection).	Implementation Validation
ISO/IEC 22237-1:2021	Information technology — Data centre facilities and infrastructures — Part 1: General concepts	This standard describes the principles for availability, reliability and resilience of data centres, seen as key element for housing and supporting IT data processing, storage and transport. Availability is also considered as a	The focus is specifically for data centre facilities and infrastructures. Although this would cover services and applications provisioned	Design Implementation

		dimension for data centres classification.	from a data centre, it does not refer to the design of generic user products.	
ITU-T X.805 (10/2003)	Security architecture for systems providing end-to-end communications	This standard defines a network security architecture for providing end-to-end network security. The architecture is applicable to different types of networks and considers several security dimensions (including availability) and security planes (management, control, end-user). The availability dimension explicitly mentions protection against active attacks such as Denial of Service (DoS).	Specific for end-to-end network security, it does not cover general aspects of systems or products design.	Design Implementation
ETSI EN 303 645 V2.1.1 (2020-06)	CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements	This standard gathers cybersecurity provisions for consumer IoT devices. It contains provisions on systems resilience to outages, including mitigations against Distributed Denial of Service (DDoS) attacks. More specifically about some provisions: 5.5 Communicate securely: Emphasizes best practice cryptography and secure authentication. 5.6 Minimize exposed attack surfaces: Focuses on disabling unused interfaces and secure development. 5.9 Make systems resilient to outages:	The provisions are expressed at high-level and target specifically consumer IoT devices.	Design Implementation

		Addresses resilience in case of data networks and power outages.		
EN IEC 62443-4-2:2019	Security for industial automation and control systems – Part 4-2: Technical security requirements for IACS components	This standard, related to IACS components, includes specific requirements focused on maintaining a baseline of operational functionalities also in cases of denial of service attacks (see Component Requirement 7.1: Denial of service protection). Moreover, it presents a requirement that prescribes a resource usage limitation capability to prevent resource exhaustion (Component Requirement 7.2: Resource management).	This standard applies only to Industrial Automation and Control System.	Design Implementation
Overall coverage and possible gaps	General availability aspects are covered by ISO/IEC 22237-1:2021 for what concerns the design of data centre facilities and infrastructures, that could be applicable to some digital products and services but do not cover all the landscape. Broader scope is provided by ISO/IEC 27002:2022 and ETSI EN 303 645 even if at a high level and, for the latter, focusing on IoT consumer devices. ITU-T X.805 (10/2003) covers the requirement for end-to-end network security. EN IEC 62443-4-2 covers the requirement for IACS. A possible gap could be the more detailed guidance on implementation of availability principles for generic user products.			

Table 8: Mapping of security requirement No. 3f

3.1.9 (3g) minimise their own negative impact on the availability of services provided by other devices or networks;

Sample Sub-requirements:

— The product should limit outgoing network connections to what is strictly needed

— The product should implement measures such as timeouts and exception handling to avoid generating multiple requests to a busy/not responsive service

Keywords: network saturation, minimization, connection limits, timeouts, exception handling

Standard ID	Standard title	Rationale	Gap	Life-Cycle
ETSI EN 303 645 V2.1.1 (2020-06)	CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements	The standard includes requirements on system resilience, limiting unnecessary exposure, and orderly network connections, which align with minimizing negative impacts on other services. Relevant Provisions: 5.6 Minimize exposed attack surfaces 5.9 Make systems resilient to outages 5.13 Validate input data	While the standard encompasses security, data protection, and resilience, it doesn't specifically focus on minimizing interference with other services as in the given requirement. Provisions related to network saturation, connection limits, and exception handling are not fully addressed in the standard, indicating potential gaps in coverage. Moreover, the provisions are expressed at high-level and target specifically consumer IoT devices.	Design Implementation
ITU-T Y.4810 (11/2021)	Requirements for data security of heterogeneous Internet of things devices	In section 9.5 "Specific requirements for data transfer to and from heterogeneous IoT devices" the following two requirements could be seen as partially covering this topic: it is required to limit the function of data transfer to and from an IoT device – the process of a specific type of data transfer is required to be initiated	Although specific, these requirements, related only to IoT devices, limit their coverage to data transfer and radio interference. In the document there are not other elements that could be mapped to this element	Design Implementation

		only with explicit permission of end users it is required to have the anti-interference ability between the IoT device and network equipment.		
Overall coverage and possible gaps	Requirement 3(g) of the CRA proposal is covered only in documents related to IoT devices, although they can be considered quite generic. However, even in these documents the coverage is limited to a minimal number of high-level provisions.			

Table 9: Mapping of security requirement No. 3g

3.1.10 (3h) be designed, developed and produced to limit attack surfaces, including external interfaces;

Sample Sub-requirements:

- The product's hardware design should limit all the connections and interfaces that are not strictly required for performing the various tasks the product is expected to do
- If required by a risk assessment, a physical product should include tamper-resistant features
- The product/service should have all not essential network ports closed as a default configuration
- Software present in digital product should be designed to avoid having unnecessary entry points (e.g. API) open and available for external unauthorised callers

Keywords: hardware hardening, tamper-resistance, system hardening, software hardening, interfaces, security by design

Standard ID	Standard title	Rationale	Gap	Life-Cycle
ISO/IEC TS 19249:2017	Information technology — Security techniques — Catalogue of architectural and design principles for secure products, systems and applications	This technical specification document describes some security design principles that would help developing a secure product. In the list it is included the attack surface minimisation principle, at the core of this requirement. The description is followed by a concrete example	This document is rather descriptive and does not include a concrete "requirements" list	Design

		of the application of the principle.		
ISO/IEC 15408-2:2022	Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 2: Security functional components	This standard lists a series of security functional components, that, in the Common Criteria jargon are defined as the basis for security functional requirements. In particular, the "Limited capabilities and availability" section defines requirements to limit the capabilities (i.e. a function should provide only the capabilities necessary for its genuine purpose) and availability (i.e. the use of a specific function should be restricted when not needed/required) of functions. This is useful to enforce design principles such as least privilege and attack surface minimization	This document does not list concrete "requirements"	Design Implementation Validation
EN IEC 62443-4-2:2019	Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components	Although this standard is specific for Industrial Automation Control Systems, it lists several requirements related to physical hardening, like "Physical tamper resistance and detection" and "use of physical diagnostic and test interfaces"	In this standard it is not present a requirement dedicated to an attack surface minimisation principle. Moreover, this document targets exclusively Industrial Automation Control Systems	Design Implementation Validation

ETSI EN 303 645 V2.1.1 (2020-06)	CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements	The requirement closely aligns with Section 5.6 of this standard, which emphasizes minimizing exposed attack surfaces through disabling unused interfaces, not unnecessarily exposing physical interfaces, and following secure development processes.	This standard is specific to IoT consumer devices and does not automatically apply to other categories of products, for which other and maybe more specific provisions may be needed.	Design Implementation
Overall coverage and possible gaps	This requirement is well covered from a theoretical point of view in the analysed documents, that well describe what are the security design principles that would allow to minimise the attack surface of a product with digital elements. Nevertheless, we found a lack of concrete requirements and practical controls that, implemented, would indeed ensure an attack surface minimisation. Standard EN IEC 62443-4-2:2019 is a partial exception to this as it included concrete requirements although limited to industrial automation and control systems.			

Table 10: Mapping of security requirement No. 3h

3.1.11 (3i) be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques;

Sample Sub-requirements:

— The product should be designed in a way that gaining unauthorised access to a function or data does not automatically lead to a complete access to all product's functions and data (defence in depth principles)

— Sensitive data stored in a product's internal memory should be encrypted at rest

— The product should not store data that is not relevant or necessary to perform its tasks (data minimisation)

Keywords: defence in depth, encryption-at-rest, data minimisation, security by design, hardening, risk assessment, secure architecture, sandboxing, secure environment

Standard ID	Standard title	Rationale	Gap	Life-Cycle
ISO/IEC 27001: 2022	Information security, cybersecurity and privacy protection — Information	Provides a systematic approach for managing information security risks.	It does not cover specific technical measures for defence in depth, encryption at rest, or sandboxing.	Design

	security management systems — Requirements			
ISO/IEC 27002: 2022	Information security, cybersecurity and privacy protection — Information security controls	Offers best practices for selecting and implementing security controls.	High-level guidelines, might lack specific details on secure software design and hardening.	Design Implementation
ISO/IEC 27034-1:2011	Information technology — Security techniques — Application security — Part 1: Overview and concepts	Focuses on secure development practices for software applications.	The standard promotes security in all software development phases, implicitly supporting defence-in-depth, but doesn't detail hardening and sandboxing. While not specifying controls like encryption at rest, it encourages risk assessments and appropriate control implementation. Data minimisation isn't explicitly addressed, but could be implemented if identified as a risk.	Design Implementation
EN ISO/IEC 15408-3:2022	Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 3: Security assurance components	Provides security evaluation criteria for IT products and systems.	This standard primarily focused on evaluation criteria, not specific mitigation mechanisms or techniques which could be enforced through security functional requirements defined in ISO/IEC 15408-2:2022.	Design Implementation

			However, it could be used to provide assurance in the product thus reducing the impact of an incident using appropriate (= assessed by the lab) exploitation mitigation mechanisms and techniques.	
EN ISO/IEC 18045: 2022	Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Methodology for IT security evaluation	Specifies the methodology for evaluating the security properties of IT products and systems.	This standard focuses on methodology for IT security evaluation, not specific mitigation mechanisms. But it supports the ISO/IEC 15408-3:2022 coverage statement above while providing evaluation methods considering for instance attack potential calculation to assess the mitigation mechanisms and techniques for robustness.	Validation
ETSI EN 303 645 V2.1.1 (2020-06)	CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements	The requirement aligns with the standard principles emphasizing secure design, encryption, minimizing data, and resilience. More specifically: Defence in Depth Principles: provisions 5.6, 5.9, and 5.6-9 cover this principle but may need more specific layering details.	Data Minimization: Lacking explicit coverage in provisions, constituting a gap. Secure architecture, sandboxing, secure environment: not explicitly defined, leading to potential gaps.	Design Implementation

		Encryption-at-Rest: provisions 5.4-1, 5.4-2, 5.3-7, and 5.5-1 partly address this requirement. Other Relevant Provisions: Ensuring software integrity (5.7) Encrypted communication (5.5) Hardening by disabling unused interfaces and minimizing code (5.6-1, 5.6-6) Secure management processes and best practice cryptography (5.5-8, 5.3-7)		
IEC 62443-3-2:2020	Security for industrial automation and control systems - Part 3-2: Security risk assessment for system design	Provides guidelines for security risk assessment and secure system design, addressing defence in depth through network segmentation strategies. It implies hardening through identification of vulnerabilities and countermeasures.	Relevant to Industrial products. While it doesn't explicitly mention encryption at rest or data minimisation, it covers security by design, risk assessment, and secure architecture. However, specific sandboxing or secure environment requirements aren't detailed.	Design
Overall coverage and possible gaps	The standards provide a solid foundation in secure system design, secure product development, risk assessment, security evaluation, and security controls. However, some aspects of defence in depth, sandboxing, and certain mitigation techniques might not be explicitly covered by the selected standards.			

Table 11: Mapping of security requirement No. 3i

3.1.12 (3j) provide security related information by recording and/or monitoring relevant internal activity, including the access to or modification of data, services or functions;

Sample Sub-requirements:

— A product should contain a log of cybersecurity related events

— Access or modification of data, services or functions should be logged

— Such log should be accessible to the privileged user

— Logs should be protected from unauthorised modification or corruption

Keywords: logging, event monitoring, non-repudiation, intrusion detection, tamper-detection

Standard ID	Standard title	Rationale	Gap	Life-Cycle
EN ISO/IEC 27002: 2022	Information security, cybersecurity and privacy protection — Information security controls	This standard provides a set of generic controls for information security risk treatment. It includes implementation guidance for the controls based on recognised best practices. Among those there is logging and monitoring activities, which embraces logging of events and protection of log information. It includes example of events to log and of unauthorised changes.	Guidance in this standard is generally provided at a high level, even though for this requirement few examples facilitate the identification of use cases and main actions to put in place.	Implementation Validation
ISO/IEC 13888-1:2020	Information security — Non-repudiation — Part 1: General	Standard specific for non-repudiation mechanisms using cryptographic techniques, it targets generation of evidence concerning relevant events. It can be applied to recording and monitoring of activities as specified in the requirement with particular focus on non-repudiation.	More general aspects not related to non-repudiation are not in the scope of this standard.	Design Implementation Validation

ETSI EN 303 645 V2.1.1 (2020-06)	CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements	Relevant Provisions: 5.9-2, 5.9-3 (Resilience): focus on resilience and restoration after outages. They imply the need to monitor system behaviour, possibly including unauthorized access attempts or modifications, although this is not explicit. 5.10-1 (Examine system telemetry data): calls for examining telemetry data, including the monitoring of system usage and behaviour. It aligns with the focus on recording and monitoring internal activities, such as unauthorized access or modifications. 5.11-1 to 5.11-4 (Easy deletion of user data): allow users to control and erase their data. They indirectly imply tracking of data access and modification 5.13-1 (Validate input data): requires data input validation to ensure its integrity and authenticity. It implies a monitoring mechanism and may indirectly relate to logging and event monitoring	The requirement related to recording and/or monitoring relevant internal activity, including the access to or modification of data, services, or functions, is not explicitly addressed. While there are some aspects related to telemetry data and input validation, specific guidelines or mandates for logging cybersecurity-related events, and ensuring that logs are accessible to privileged users while being protected from unauthorized modification or corruption, are not expressly detailed in the standard.	Design Implementation Validation Surveillance Maintenance
IEC 62443-4-2:2019	Security for industrial automation and control systems - Part 4-2: Technical security requirements	This standard is related to IACS. Within the listed requirements there are also provisions about event auditing (Component Requirement 2.8: Auditable events), timestamping of audit	Relevant only to IACS.	Design Implementation

	for IACS components	records (Component Requirement 2.11: Timestamps) and non-repudiation (Component Requirement 2.12: Non-repudiation)		
Overall coverage and possible gaps	Monitoring aspects with specific focus on non-repudiation are covered in ISO/IEC 13888-1:2020. ISO/IEC 27002:2022 gives a more general overview and high-level provisions. ETSI EN 303 645 V2.1.1 touches upon telemetry data, data validation and integrity. EN 62443-4-2 covers the requirement for IACS.			

Table 12: Mapping of security requirement No. 3j

3.1.13 (3k) ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic updates and the notification of available updates to users.

Sample Sub-requirements:

— The company distributing a product or service should provide timely security updates for the software components of the product/service for a reasonable amount of time.

— A function to automatically check the presence of updates and install them, or notify the user of their presence, should be implemented, and where applicable this should be the default initial configuration.

— A product should provide a secure mechanism to install/implement updates

— The company distributing a product should notify the user on the availability of updates

Keywords: Indicator of Compromise, patching, software updates, automatic updates, user notification, secure update functionality

Standard ID	Standard title	Rationale	Gap	Life-Cycle
EN ISO/IEC 27002: 2022	Information security, cybersecurity and privacy protection — Information security controls	Covers general principles for information security management, including patch management	Lacks specific guidance on automatic updates and user notifications	Design Validation
ISO/IEC 30111: 2019	Information technology — Security techniques — Vulnerability handling processes	Focuses on vulnerability handling processes but not specifically on the mechanisms for delivering and installing updates	Lacks guidance on secure mechanisms for installing/implementing updates	Design

ETSI EN 303 645 V2.1.1 (2020-06)	CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements	Addresses security updates, automatic updates, and user notifications for consumer IoT devices	Lacks detailed guidance on secure mechanisms for installing/implementing updates	Design
IEC 62443-2-1:2010	Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program	Addresses patch management and updates in the context of industrial automation and control systems	Limited to industrial automation and control system environments. It does not cover automatic updates and user notifications in detail	Design
IEC 62443-4-2:2019	Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components	Provides guidance on patch management and security updates for IACS components	Limited to industrial automation and control system components – It does not cover user notifications	Design
Overall coverage and possible gaps	The identified standards focus on different aspects of vulnerability management, patching, and updates. However, some standards mention the need for secure updates, but they do not provide detailed guidance on the secure mechanisms for installing/implementing updates. Also, they do not explicitly cover the requirement of notifying users about the availability of updates.			

Table 13: Mapping of security requirement No. 3k

3.2 Vulnerability handling requirements

3.2.1 Manufacturers of the products with digital elements shall: (1) 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;

Sample Sub-requirements:

- A monitoring of the cybersecurity status of the overall supply chain for the acquisition of the necessary components incorporated in the product should be put in place.
- All libraries and external components used in the software part of a product, including their version number should be listed in a Software Bill of Material (SBOM) available to the user
- Such Software bill of materials (SBOM) should be compliant to the relevant standards (e.g., ISO/IEC 5921:2021 also known as SPDX [2] or CycloneDX [4] standard)

Keywords: software bill of materials, SPDX, CycloneDX, supply chain security, machine-readable, versioning, software dependencies, composability

Standard ID	Standard title	Rationale	Gap	Life-Cycle
ISO/IEC 27036 **Parts 1 to 3**	Cybersecurity — Supplier relationships — Part 1:2021 Overview and concepts Cybersecurity — Supplier relationships — Part 2:2022 Requirements Cybersecurity — Supplier relationships — Part 3: Guidelines for hardware, software, and services supply chain security	This standard covers information security for supplier relationships. It provides guidance on managing information security risks associated with suppliers and third-party developers. This can be relevant to SBOM in the context of the software supply chain.	While it is relevant to the overall supply chain, it doesn't specifically address the creation, management, or exchange of Software Bill of Materials (SBOM).	Design Surveillance Maintenance
Overall coverage and possible gaps	To address the gaps in ISO/IEC 27036 related to Software Bill of Materials (SBOM), it's recommended to consider the following standards and initiatives: — SPDX: A Linux Foundation standard for sharing software components, licenses, copyrights, and security data, providing a consistent SBOM format [2].			

	— NTIA's Software Component Transparency Initiative: A U.S. initiative working on standardizing SBOM formats and best practices for software component transparency [3]. — CycloneDX: An SBOM specification designed for application security and supply chain component analysis, offering a lightweight format for describing software components and metadata [4]. — ECSO Supply Chain management and Product Certification Composition [5] — IIoTSBOM is an initiative from LSEC, Flanders Make and KU Leuven COSIC from Belgium to improve cybersecurity for devices. Inspired and with the support of the US CISA (Cyber Security and Infrastructure Security Agency) [6] Combining these standards and initiatives with ISO/IEC 27036 can help create a comprehensive approach to managing SBOMs, addressing information security risks in supplier relationships, and improving software supply chain transparency.

Table 14: Mapping of vulnerability handling requirement No. 1

3.2.2 (2) in relation to the risks posed to the products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates;

Sample Sub-requirements:

— In case vulnerabilities are found they should be classified in accordance with standard severity metrics (e.g. CVSS)

— vulnerabilities that can be directly fixed by the company should be fixed without delay, in accordance to their severity and the posed risks

— In case a vulnerability is found in a software component of a product (including libraries and third party components), an update should be prepared and distributed as soon as possible

— The company developing a product or service should be subscribed to updates coming from CERTs and cybersecurity organisations and analyse them in order to spot vulnerabilities in their products

— The company developing a product or service should remain updated on the release of new versions of the libraries or third party software components included in their products/services and update the relative software whenever such new version includes a security update

Keywords: security updates, CVSS, updates release, vulnerability management, secure policy

Standard ID	Standard title	Rationale	Gap	Life-Cycle
ISO/IEC 27001: 2022	Information security, cybersecurity and privacy protection — Information security management	This international standard provides a framework for establishing, implementing, maintaining, and continually improving an information	This standard provides a high-level framework for information security management. It doesn't explicitly cover vulnerability classification, patch	Surveillance Maintenance

	systems — Requirements	security management system (ISMS). It outlines the requirements for managing risks related to information security, including addressing and remediating vulnerabilities in digital products.	management, or handling security updates for libraries and third-party components.	
ISO/IEC 27002: 2022	Information security, cybersecurity and privacy protection — Information security controls	This standard provides best practices and guidelines for implementing information security controls in organizations. It covers various aspects of vulnerability management, including risk assessment, vulnerability classification, and remediation.	While it offers guidelines for information security controls, it is not sufficient in providing detailed guidance on vulnerability classification, specific patch management procedures, or addressing vulnerabilities in third-party components.	Surveillance Maintenance
EN ISO/IEC 30111: 2020	Information technology — Security techniques — Vulnerability handling processes	This standard specifies the process for vulnerability handling in software products. It provides guidance on how organizations can identify, analyse, and remediate vulnerabilities in their software products, including distributing security updates.	This standard focuses on the process for vulnerability handling in software products but does not specifically address subscribing to updates from CERTs and cybersecurity organizations or maintaining updates for third-party components and libraries.	Surveillance Maintenance
EN ISO/IEC 29147: 2020	Information technology — Security techniques —	This standard defines the process for vulnerability disclosure, focusing on how organizations can receive and	This standard focuses on vulnerability disclosure and does not cover aspects like vulnerability classification,	Surveillance Maintenance

	Vulnerability disclosure	process vulnerability reports from external sources, such as CERTs and cybersecurity organizations.	remediation, and patch management in a comprehensive manner.	
EN IEC 62443-4-1 2018	Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements	This standard is related to IACS. It contains requirements covering security updates and in particular timely delivery of security patches (SUM-1 "Security update qualification" and SUM-5 "Timely delivery of security patches")	This standard is for IACS only. Moreover, although it requires security patches, it does not cover aspects like vulnerability classification, remediation and patch management in a comprehensive manner.	Surveillance Maintenance
Overall coverage and possible gaps	While each standard provides valuable information and guidance, there is no single standard that comprehensively addresses all aspects of vulnerability management, including classification, remediation, patch management, handling updates from CERTs and cybersecurity organizations, and maintaining updates for third-party components and libraries. To cover this gap, these standards could be combined to address the specific security needs aligned with sectoral requirements, and the regulatory landscape. By leveraging the strengths of each standard, a more comprehensive vulnerability management process addressing and remediating vulnerabilities in products with digital elements could be needed to fully cover this requirement.			

Table 15: Mapping of vulnerability handling requirement No. 2

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

Sample Sub-requirements:

- Periodic vulnerability assessment should be executed, especially towards those components that present the highest risk
- When developing or maintaining software components, automatic tests should be executed whenever a new commit/build/version is prepared, if possible using Continuous Integration/Continuous Deployment (CI/CD) techniques
- A risk assessment should be re-evaluated whenever there is a significant change in one of the dimensions analysed (new threats, new vulnerabilities, etc.) or a new product release.

Keywords: vulnerability assessment, continuous integration/continuous deployment, risk assessment, security testing procedures, testing

Standard ID	Standard title	Rationale	Gap	Life-Cycle
ISO/IEC 27001: 2022	Information security, cybersecurity and privacy protection — Information security management systems — Requirements	This international standard provides a framework for establishing, implementing, maintaining, and continually improving an information security management system (ISMS). It outlines the requirements for managing risks related to information security, including performing regular security tests and reviews.	This standard provides a high-level framework for information security management. It does not explicitly cover detailed security testing procedures, continuous integration/continuous deployment (CI/CD), or specific testing methodologies.	Surveillance Maintenance
ISO/IEC 27002: 2022	Information security, cybersecurity and privacy protection — Information security controls	This standard provides best practices and guidelines for implementing information security controls in organizations. It covers various aspects of security testing and vulnerability management, including risk assessment and periodic reviews.	While it offers guidelines for information security controls, it is not sufficient in providing detailed guidance on specific security testing procedures, CI/CD techniques, or the frequency and scope of testing.	Surveillance Maintenance
ISO/IEC TS 27034-5-1:2018	Information technology — Application security — Part 5-1: Protocols and application security controls data structure, XML schemas	This standard focuses on application security and provides guidelines for embedding security into the software development lifecycle, including regular security testing and reviews of applications.	This standard focuses on application security but might not cover all aspects of security testing, especially for non-software products, hardware components, or infrastructure elements.	Surveillance Maintenance

ISO/IEC 27005: 2022	Information security, cybersecurity and privacy protection — Guidance on managing information security risks	This standard provides guidelines for information security risk management, which includes risk assessment, risk treatment, and regular monitoring and review of risks associated with digital products.	This standard provides guidelines for information security risk management, but it does not cover specific security testing methodologies or CI/CD techniques.	Surveillance Maintenance
Overall coverage and possible gaps	While each standard provides valuable information and guidance, there is no single standard that comprehensively addresses all aspects of security "effective" testing and reviews for products with digital elements, including specific testing methodologies, CI/CD techniques, and the frequency and scope of testing. To cover this gap, it could be considered the implementation of a combination of these standards and guidelines, tailoring the approach to the specific needs, industry, and regulatory landscape. By leveraging the strengths of each standard, it may be developed a more comprehensive security testing process during the development phase (e.g. DevSecOps) that addresses the requirement of applying effective and regular tests and reviews of the security of products with digital elements.			

Table 16: Mapping of vulnerability handling requirement No. 3

3.2.4 (4) once a security update has been made available, publically 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 information helping users to remediate the vulnerabilities;

Sample Sub-requirements:

— New CVE indicators should be publicly released and disseminated as soon as the relative security update has been released or implemented

Keywords: Common Vulnerabilities and Exposures (CVE), vulnerability disclosure, vulnerability analysis

Standard ID	Standard title	Rationale	Gap	Life-Cycle
EN ISO/IEC 29147: 2020	Information technology — Security techniques — Vulnerability disclosure	This standard provides guidelines for vulnerability disclosure, including recommendations on how to disclose	This standard provides guidelines for vulnerability disclosure but does not offer	Surveillance Maintenance

		vulnerability information, such as the nature of the vulnerabilities, affected products, impacts, severity, and remediation information.	specific guidance on the timeline for public disclosure or the exact format for sharing vulnerability information.	
EN ISO/IEC 30111: 2020	Information technology — Security techniques — Vulnerability handling processes	This standard focuses on the process of vulnerability handling in software products, including the steps necessary to investigate, resolve, and publicly disclose vulnerability information.	While it focuses on the process of vulnerability handling in software products, it does not provide detailed guidance on the public disclosure of vulnerability information for non-software products or hardware components.	Surveillance Maintenance
ETSI EN 303 645 V2.1.1 (2020-06)	CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements	This European standard is dedicated to consumer internet of things. Chapter 5.2 is dedicated to a means to manage reports of vulnerabilities. It refers to EN ISO/IEC 29147 document.	Even if the standard remains quite generic it is dedicated to internet of things (IoT). It provides overview of vulnerability disclosure policy content, timeline is a general one and not more precise than EN ISO/IEC 29147.	Surveillance Maintenance
EN IEC 62443-4-1 2018	Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements	This standard is related to IACS. Requirement DM-5 “Disclosing security-related issues” prescribes the disclosure of information related to the fixed vulnerability in a timely matter.	This standard is for IACS only.	Surveillance Maintenance

Overall coverage and possible gaps	While these standards and initiatives contribute to the process of vulnerability disclosure, they do not comprehensively address all aspects of public disclosure, such as specific disclosure timelines or the exact format for sharing vulnerability information across different industries or product types. To cover this gap, it could be considered the implementation of a combination of these standards and initiatives, tailoring the approach to the specific needs, industry, and regulatory landscape. Additionally, it may be possible to rely on vulnerability disclosure policies and procedures that align with industry best practices (including for instance: CVE [7], NIST National Vulnerability Database (NVD) [8], FIRST Vulnerability Reporting and Data eXchange (VRDX) SIG [9]). As part of a holistic approach, engaging with and incorporating feedback from various stakeholders, such as customers, researchers, and security experts, should be an ongoing, integral part of the vulnerability management process. By leveraging the strengths of each standard and initiative, it may be possible to create a comprehensive and effective vulnerability disclosure process that meets the requirement and its sub-requirements.

Table 17: Mapping of vulnerability handling requirement No. 4

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

Sample Sub-requirements:

— The company should adopt and enforce the CVD policy

Keywords: CVD policy

Standard ID	Standard title	Rationale	Gap	Life-Cycle
EN ISO/IEC 29147: 2020	Information technology — Security techniques — Vulnerability disclosure	This standard provides guidelines for vulnerability disclosure, which includes recommendations for organizations to develop and implement a CVD policy. It offers guidance on the disclosure process, roles and responsibilities, and how to communicate vulnerability information.	This standard offers guidelines for vulnerability disclosure but does not provide detailed guidance on the implementation of a CVD policy, such as specific processes or requirements for different industries.	Design Surveillance Maintenance
EN ISO/IEC 30111: 2020	Information technology — Security techniques — Vulnerability	This standard focuses on the process of vulnerability handling in software products. It complements ISO/IEC 29147 by providing	This standard is dedicated to vulnerability handling processes, including	Design Surveillance Maintenance

	handling processes	guidance on investigating, resolving, and disclosing vulnerabilities in a coordinated manner.	coordinated vulnerability disclosure (CVD). However, it doesn't specify the enforcement of a particular national or EU CVD policy.	
ETSI EN 303 645 V2.1.1 (2020-06)	CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements	This European standard is dedicated to consumer internet of things. Chapter 5.2 is dedicated to a means to manage reports of vulnerabilities. It refers to EN ISO/IEC 29147 document	Even if the standard remains quite generic it is dedicated to internet of things (IoT). It provides some details related to vulnerability disclosure, and highlights the successful use of CVD in some software industries but without details on how to apply it in the IoT domain. There is also a reference to the Common Vulnerability Reporting Framework (CVRF) but without details.	Surveillance Maintenance
Overall coverage and possible gaps	While the mentioned standards and initiatives contribute to the development and implementation of a CVD policy, they do not comprehensively address all aspects of enforcing such a policy or provide specific guidance tailored to different industries and product types. To cover this gap, it could be considered the implementation of a combination of these standards, initiatives, and national / EU CVD policies. Additionally, it may be possible to rely on CVD policies and procedures that align with industry best practices (e.g. NIST SP 800-61 Revision 2 [10], FIRST VRDX SIG [9]). By leveraging the strengths of each standard and initiative, it may be possible to create a comprehensive and effective CVD policy that meets the requirement.			

Table 18: Mapping of vulnerability handling requirement No. 5

3.2.6 (6) 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;

Sample Sub-requirements:

— The company distributing a product/service should have a contact point specifically advertised to collect information related to vulnerabilities found in their products/services. If the company has one, this contact point should be the company's PSIRT

— The company distributing a product/service should inform any relevant authority (e.g. national CERT/CSIRT) about how they can be reached in a timely manner for reasons related to the handling of vulnerabilities

Keywords: PSIRT, discovered vulnerabilities

Standard ID	Standard title	Rationale	Gap	Life-Cycle
EN ISO/IEC 29147: 2020	Information technology — Security techniques — Vulnerability disclosure	This standard provides guidelines for vulnerability disclosure, including recommendations on how organizations can establish and maintain communication channels for reporting vulnerabilities. It covers the roles and responsibilities of organizations and the process for communicating vulnerability information.	This standard provides guidelines for vulnerability disclosure but does not specifically address the sharing of information about potential vulnerabilities in third-party components.	Design
EN ISO/IEC 30111: 2020	Information technology — Security techniques — Vulnerability handling processes	This standard focuses on the process of vulnerability handling in software products, which can be extended to cover digital elements and third-party components. It complements ISO/IEC 29147 by providing guidance on investigating, resolving,	Focused on vulnerability handling in software products, it does not comprehensively cover the aspects of sharing information about potential vulnerabilities in third-party components and other digital elements.	Design

		and disclosing vulnerabilities.		
Overall coverage and possible gaps	The mentioned standards and initiatives contribute to various aspects of the requirement but do not comprehensively address sharing information about potential vulnerabilities in third-party components and other digital elements. To cover this gap, it could be considered the implementation of a combination of these standards, initiatives, and collaborate with national CERTs/CSIRTs and ENISA. It may be possible to also follow the CSIRTs Network forum and [11] latest ENISA activities on that topic under the EU Cybersecurity Act umbrella. The CSIRTs Network is composed of CSIRTs appointed by EU Member States and CERT- EU ('CSIRTs Network members'). It is worth noting that ENISA actively supports cooperation between CSIRTs, provides the secretariat and supports incident coordination upon request. Additionally, it may be possible to rely on policies and procedures that align with industry best practices (e.g., NIST SP 800-61 Revision 2 [10], FIRST PSIRT Services Framework [12]). By leveraging the strengths of each standard and initiative, it may be possible to create a comprehensive and effective process for sharing information about potential vulnerabilities and handling discovered vulnerabilities in their products with digital elements and third-party component.			

Table 19: Mapping of vulnerability handling requirement No. 6

3.2.7 (7) provide for mechanisms to securely distribute updates for products with digital elements to ensure that exploitable vulnerabilities are fixed or mitigated in a timely manner;

Sample Sub-requirements:

— Security updates should be digitally signed using a Code Signing Certificate to ensure the identity of the issuer

— Hashes of the updates should be made publicly available with instructions on how to verify them

Keywords: code signing certificate, hashing, secure software update distribution, digital signatures, official distribution channel, hash publication

Standard ID	Standard title	Rationale	Gap	Life-Cycle
ISO/IEC 27002: 2022	Information security, cybersecurity and privacy protection — Information security controls	This standard provides guidelines for information security controls, including secure software distribution and update management. It covers aspects such as securing development environments,	Although it provides guidelines for secure software distribution, it does not explicitly address the requirement of publishing hashes of updates and providing	Design

		cryptographic controls, and securing distribution channels.	instructions for verification.	
IEC 62443-4-1:2018	Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements	This standard focuses on defining process requirements for the secure development of products used in industrial automation and control systems. It covers security requirements throughout the product development lifecycle, including design, implementation, testing, and maintenance. While the standard is primarily targeted at the development of secure products, it also addresses aspects related to secure software updates and patch management, which are important for securely distributing updates.	While IEC 62443-4-1 addresses security aspects throughout the product development lifecycle, including aspects related to secure software updates and patch management, there are potential gaps when it comes to covering the analysed requirement of securely distributing updates for products with digital elements. Industry specificity: IEC 62443-4-1 is tailored to Industrial Automation and Control Systems (IACS). Although the standard's principles can be applied to other industries, it does not fully cover the unique needs and challenges of other sectors. Explicit mention of hashes and verification: The standard does not explicitly address the publication of update hashes and the provision of instructions for verifying them. Organizations may need to develop additional guidelines or policies to ensure that hashes are published and that users receive clear instructions for verifying the authenticity and	Design

			integrity of software updates. Code signing certificate: While the standard covers secure software development practices, it does not explicitly mention the requirement of using code signing certificates to sign security updates, which ensures the identity of the issuer and the integrity of the update.	
Overall coverage and possible gaps	The mentioned standards contribute to various aspects of the requirement but does not comprehensively address the publication of update hashes and the provision of instructions for their verification. To cover this gap, it could be considered the implementation of a combination of these standards, tailored to the specific needs and industry best practices (e.g., NIST SP 800-53 [13], NIST SP 800-63B [14], OWASP SSDLC [15]). It may be possible to take a closer look into the Patch Management mechanism suggest in the EUCC [16]. The latter provides a framework for securely distributing updates for products with digital elements, ensuring that exploitable vulnerabilities are fixed or mitigated in a timely manner. By leveraging the strengths of each standard and considering input from various sources, it may be possible to create a comprehensive and effective process for securely distributing updates and mitigating exploitable vulnerabilities in a timely manner.			

Table 20: Mapping of vulnerability handling requirement No. 7

3.2.8 (8) ensure that, where security patches or updates are available to address identified security issues, they are disseminated without delay and free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken.

Sample Sub-requirements:

- Users should be made aware of the existence of security updates either via automatic distribution, popup, newsletter, etc.
- This notice should contain information about the fixed issues and instructions on how to apply the update
- Security updates should be released free of charge

Keywords: Security update notice

Standard ID	Standard title	Rationale	Gap	Life-Cycle
EN ISO/IEC 30111: 2020	Information technology — Security techniques — Vulnerability handling processes	This standard provides guidelines for the design and implementation of vulnerability handling processes, including the discovery, reporting, and remediation of vulnerabilities. It can help organizations develop processes to ensure timely dissemination of security patches, updates, and advisories	While the standard covers vulnerability handling processes, it does not explicitly address the requirement of providing security updates free of charge or specific methods for notifying users.	Surveillance Maintenance
ISO/IEC 27002: 2022	Information security, cybersecurity and privacy protection — Information security controls	This standard provides best practice recommendations on information security management for organizations. Section 12.6, "Technical Vulnerability Management," covers aspects related to vulnerability management, including the timely application of security patches and updates.	This standard provides best practice recommendations but does not provide explicit guidance on providing updates free of charge or specific notification methods for users.	Surveillance Maintenance
EN IEC 62443-4-1 2018	Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements	This standard is related to IACS. Requirements DM-5: “Disclosing security-related issues” and SUM-5 “Timely delivery of security patches” cover the requirement with the notable exception of the gratuitousness if the security update	This standard is for IACS only. Moreover, it does not make explicit that the security update should be free of charge	Surveillance Maintenance

Overall coverage and possible gaps	The existing standards and guidelines generally provide guidance on vulnerability management, patch management, and the dissemination of security updates. However, they do not explicitly address certain aspects of the requirement, such as providing updates free of charge or specifying methods for user notification. To cover the overall gap, it could be possible to define policies that mandate providing updates free of charge and establishing specific methods for notifying users about available security updates.

Table 21: Mapping of vulnerability handling requirement No. 8

4 Summary of the identified standards and overall remarks

Here the overall list of identified standards is summarised with the respective mapping, grouping them according to the two groups of CRA essential requirements.

	Security requirements relating to the properties of products with digital elements												
Standard	**1**	**2**	**3 a**	**3 b**	**3 c**	**3 d**	**3 e**	**3 f**	**3 g**	**3 h**	**3 i**	**3 j**	**3 k**
EN ISO/IEC 27002:2022	x		x					x			x	x	x
EN ISO/IEC 27005:2022	x												
EN IEC 62443-3-2:2020	x										x		
EN IEC 62443-4-1:2018	x	x											
ISO/IEC 18045:2022		x									x		
ITU-T X.1214 (03/2018)		x											
ETSI EN 303 645 V2.1.1 (2020-06)	x	x	x	x	x	x	x	x	x	x	x	x	x
ISO/IEC 18031:2011			x										
ISO/IEC 9798, Parts 1 to 6				x									
ISO/IEC 24760, Parts 1 to 3				x									
ISO/IEC 29146:2016				x									
ITU-T X.1253 (09/2011)				x									
ITU-T X.812 (11/1995)				x									
EN IEC 62443-4-2:2019				x	x	x		x		x		x	x
ITU-T X.805 (10/2003)					x			x					
ISO/IEC 18033, Parts 1 to 7					x								
ITU-T X.814 (11/1995)					x								
ISO/IEC 9796, Parts 2 and 3						x							
ISO/IEC 9797, Parts 1 to 3						x							
ISO/IEC 14888, Parts 1 to 3						x							

ITU-T X.815 (11/1995)						x							
ISO/IEC 27701:2019							x						
ISO/IEC 29100:2011							x						
ETSI TS 103 485 V1.1.1 (2020-08)							x						
ISO/IEC 22237-1:2021								x					
ITU-T Y.4810 (11/2021)									x				
ISO/IEC TS 19249:2017										x			
ISO/IEC 15408-2:2022										x			
ISO/IEC 27001:2022											x		
ISO/IEC 27034-1:2011											x		
EN ISO/IEC 15408-3:2022											x		
ISO/IEC 13888-1:2020												x	
ISO/IEC 30111:2019													x
IEC 62443-2-1:2010													x

Table 22: Overall list of the identified standards with their respective mapping towards the security requirements

	Vulnerability handling requirements							
Standard	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
ISO/IEC 27036, Parts 1 to 3	x							
ISO/IEC 27001:2022		x	x					
ISO/IEC 27002:2022		x	x				x	x
EN ISO/IEC 30111:2020		x		x	x	x		x
EN ISO/IEC 29147:2020		x		x	x	x		
IEC 62443-4-1:2018		x		x			x	x
ISO/IEC TS 27034-5-1:2018			x					

ISO/IEC 27005:2022			x					
ETSI EN 303 645 V2.1.1 (2020-06)				x	x			

Table 23: Overall list of the identified standards with their respective mapping towards the vulnerability handling requirements

Some overall remarks stem from the detailed analysis of the previous section and from the two above summary tables, and are summarized here below:

- Overall, the existing standards cover at least partially all CRA requirements. This provides a strong basis to build on taking into consideration the identified gaps. Nevertheless, we did not find a single standard that can, alone, satisfy all requirements listed in the two lists present in Annex I of the CRA;
- In general, "horizontal" standards - i.e., not targeting a specific use case or a market sector - emerged as the most relevant to cover the purposes of the different requirements. The only exception to this is represented by some standards of the EN IEC 62443 family (related to industrial control systems) and the Internet of Things (IoT), although in our opinion standards targeting the IoT domain can be seen mostly as horizontal standards, since nowadays most digital devices can be associated to the IoT scenario;
- Although some of the selected standards are not directly related to product design/development (e.g., EN ISO/IEC 27002 related to recommended controls for initiating, implementing or maintaining information security management systems), they might nevertheless be relevant for the CRA, as their implementation by an organisation will be reflected also in the products produced by that organisation;
- Regarding the product-related security requirements of the first list of CRA Annex I, the standard ETSI EN 303 645 has been indicated to us as one of the most relevant, and for this reason we have made a specific attempt to map it on all the requirements, which result somehow all covered by the standard even if with some gaps. To be also noted that the standard is specifically devoted to IoT systems, so, even if many digital products nowadays present different features analogous to those of the IoT environment, an automatic applicability of this standard to all categories of products cannot to be taken for granted (see also the comment below about the requirement 3g). Another relevant standard in terms of coverage of the requirements is EN ISO/IEC 27002 (information security controls), covering 6 out of 13 requirements. Also the EN IEC 62443 family offers a quite good coverage, but it is specifically devoted to industrial control systems.
- For the vulnerability handling requirements, the second list of the annex, EN ISO/IEC 30111 (vulnerability handling process) is the most relevant one, covering 5 out of 8 requirements, with also EN ISO/IEC 29147 (vulnerability disclosure) covering 4 of the same requirements. All these standards are "horizontal" in terms of their application;
- In some cases, such as requirement 3(b) (*ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems*), the selected standards are quite generic whereas there exist several other standards covering specific use cases in more detail. The selection of more generic standards allows more flexibility and wider coverage of current and future use cases. On the other hand, specific and sectoral standards might be able to satisfy more closely the peculiar constraints and requirements of specific niches;

— In other cases, e.g., 3(f) (*protect the availability of essential functions, including the resilience against and mitigation of denial of service attacks*), the focus of the identified documents is more on infrastructural elements rather than user products or services. Even though these infrastructures are the core for provisioning of services and for some device functionalities, more specific standard provisions would be needed. Those are present for IoT devices, but still at a high level;

— While requirement 3(g), which focuses on *minimizing negative impacts on the availability of services provided by other devices or networks*, is specifically addressed by standards related to the IoT domain, it raises questions about the broader applicability of these standards. In the context of the highly interconnected nature of devices in the IoT domain, these standards have clear relevance. However, for other domains, the specific applicability of IoT-focused cybersecurity standards may need further evaluation. While interconnectedness is also a characteristic of several domains nowadays, the specific requirements, regulations, and risks might vary, necessitating a tailored approach or additional measures to ensure that cybersecurity needs are adequately addressed.

5 Conclusion

Products with digital elements are evermore present in our lives. The increasing number of cyberattacks affecting them triggers negative impacts on many different aspects of our society. As a response the European Commission has proposed the Cyber Resilience Act, a new legislative framework prescribing a set of cybersecurity requirements that manufacturers have to implement in their products with digital elements.

The defined requirements should be translated into harmonised European standards which would become the reference cybersecurity specifications to be followed by manufacturers. In view of this standardisation activity, this report identifies the most relevant already existing cybersecurity standards mapping them to the different requirements, describing both the level of offered coverage and the gaps to be possibly considered in further standardisation efforts.

According to our analysis for each of the defined requirements there is already at least one document that can be considered as an initial reference offering some coverage. However, to the best of our knowledge, there is not a single standard capable of covering all the requirements expressed in the proposed legislative act, even if some of the standards do partially cover all of the requirements. The analysis offers re-assurance that a good international cybersecurity standardisation base is already in place for serving the scope of the Cyber Resilience Act requirements, but harmonisation is needed to ensure a homogeneous horizontal coverage, and some gaps, as highlighted in this report, need still to be addressed.

References

[1] 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. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0454

[2] SPDX: A Linux Foundation standard for sharing software components, licenses, copyrights, and security data, providing a consistent SBOM format - SPDX Specification 2.2. https://spdx.github.io/spdx-spec/

[3] NTIA's Software Component Transparency Initiative - a U.S. initiative working on standardizing SBOM formats and best practices for software component transparency. https://www.ntia.gov/SBOM

[4] CycloneDX: An SBOM specification designed for application security and supply chain component analysis, offering a lightweight format for describing software components and metadata - CycloneDX Specification. https://cyclonedx.org/capabilities

[5] ECSO Supply Chain management and Product Certification Composition. https://ecs-org.eu/activities/standardisation-certification-and-supply-chain-management/

[6] IIoTSBOM is an initiative from LSEC, Flanders Make and KU Leuven COSIC from Belgium to improve cybersecurity for devices. Inspired and with the support of the US CISA (CyberSecurity and Infrastructure Security Agency). https://www.iiotsbom.com/

[7] The Common Vulnerabilities and Exposures (CVE) system provides a reference-method for publicly known information-security vulnerabilities and exposures. https://cve.mitre.org/

[8] The National Vulnerability Database (NVD) is the U.S. government repository of standards-based vulnerability management data, enabling automation of vulnerability management, security measurement, and compliance. https://www.nist.gov/itl/products-and-services/national-vulnerability-database-nvd

[9] The Vulnerability Reporting and Data eXchange Special Interest Group (VRDX SIG) of the Forum of Incident Response and Security Teams (FIRST) focuses on improving vulnerability management processes and standards. https://www.first.org/global/sigs/vrdx

[10] NIST SP 800-61 Revision 2 - Computer Security Incident Handling Guide. https://www.researchgate.net/publication/320851514_NIST_Special_Publication_800-61_Revision_2_Computer_Security_Incident_Handling_Guide

[11] The CSIRT (Computer Security Incident Response Team) Network is a collaborative platform where members can cooperate, exchange information, and build trust. The network's members, composed of CSIRTs appointed by EU Member States and CERT-EU ('CSIRTs Network members'), work together to improve the handling of cross-border incidents and discuss how to respond in a coordinated manner to specific incidents. https://www.enisa.europa.eu/topics/incident-response/csirts-in-europe/csirts-network

[12] The PSIRT (Product Security Incident Response Team) Services Framework is a document developed by the FIRST (Forum of Incident Response and Security Teams) community, detailing potential services that CSIRTs (Computer Security Incident Response Teams) and PSIRTs may provide. https://www.first.org/resources/guides/first-psirt-services-framework-v1.0.pdf

[13] NIST SP 800-53: This standard provides a catalog of security and privacy controls for all U.S. federal information systems except those related to national security. It aims to protect individuals' privacy and organizational operations from a diverse set of threats. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

[14] NIST SP 800-63B: This is a guideline for digital identity services. It offers technical requirements for each of three levels of assurance in the areas of identity proofing,

authentication, and federation. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf

[15]OWASP SSDLC: The Open Web Application Security Project (OWASP) Secure Software Development Life Cycle Project is a guide to security in the software development life cycle. It provides a core framework for integrating security concepts and best practices into a software development process. https://owasp.org/www-project-secure-software-development-lifecycle/

[16]The patch management approach outlined in the EU Common Criteria is for certified ICT products and aims to ensure the security of the products through proper vulnerability handling and patch deployment. The process allows for different patch levels based on the severity and urgency of vulnerabilities, and it involves the collaboration of various stakeholders in the certification process. Annex 15: https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme-v1-1.1

List of abbreviations and definitions

API	Application Programming Interface
CERT	Computer Emergency Response Team
CD	Continuous Deployment – A Software engineering approach that involves regularly delivering software features using automated deployment processes.
CI	Continuous Integration – A Software engineering approach that consists in automatically integrating code changes from various contributors into a unified software repository, where automated tests and builds are performed.
CISA	Cybersecurity and Infrastructure Security Agency - A U.S. government agency responsible for cybersecurity and critical infrastructure protection
CRA	Cyber Resilience Act
CSIRT	Computer Security Incident Response Team
CVD	Coordinated Vulnerability Disclosure - A process of reporting and addressing vulnerabilities in a collaborative manner
DoS	Denial of Service
DDoS	Distributed Denial of Service
ECSO	European Cyber Security Organisation - An organization that aims to develop a cybersecurity ecosystem in Europe
ENISA	European Union Agency for Cybersecurity
ESO	European Standardisation Organization
FIRST	Forum of Incident Response and Security Teams - A global organization focused on incident response and security coordination
GDPR	General Data Protection Regulation
IACS	Industrial Automation and Control Systems
IIoTSBOM	Industrial Internet of Things Software Bill of Materials - An initiative to improve cybersecurity for devices
IoT	Internet of Things
ISMS	Information Security Management System
JRC	Joint Research Centre

LSEC	Leaders in Security - A European information security cluster
NIST	National Institute of Standards and Technology - A U.S. government agency that develops standards and guidelines
NTIA	National Telecommunications and Information Administration - A U.S. government agency
PII	Personal Identifiable Information
PKI	Public Key Infrastructure
PSIRT	Product Security Incident Response Team - A team responsible for handling security incidents and vulnerabilities in products
ROM	Read Only Memory
SaaS	Software as a Service
SBOM	Software Bill of Materials - A document that lists the components used in a software product
SDO	Standards Developing Organisation
SP	Special Publication - A series of publications by NIST covering various technology and security topics
SPDX	Software Package Data Exchange - A Linux Foundation standard for sharing software component information
VRDX SIG	Vulnerability Reporting and Data eXchange Special Interest Group - A group within FIRST focused on vulnerability reporting and data exchange
XML	eXtensible Markup Language

List of figures

List of Tables

Annexes

Annex 1. High level pre-screening of standardisation activities with potential relevance for the CRA requirements

As preparatory activity of the present study, with the aim to offer a robust mapping of the CRA requirements against the relevant cybersecurity standardisation activities offered by European and international standardisation body, several outputs produced by their committees have been surveyed. This pre-analysis has represented the ground on which to build the detailed mapping of standards against the CRA requirements.

In the screening activity already published standards have been obviously considered, but ongoing standardisation efforts, technical specifications, technical reports and guidelines have been also taken into consideration. The analysis of each of them has been based solely on freely available information, like overviews, summaries, abstracts, tables of content and where possible the full text. For each identified document a tentative coarse mapping against the CRA requirements has been sketched, so as to measure the potential relevance of each of them in the actual mapping.

In the table below we summarise the number of committees and documents we went through for the pre-screening of the present study, so as to give an insight about the amplitude of the analysis.

	Committees/Working groups	**Surveyed Standards/Documents**
International SDOs (ISO, IEC, ITU)	37	~ 950
European SDOs (CEN, CENELEC, ETSI)	25	~ 270

Table 1 Number of committees/working groups and standards/documents considered in the analysis.

GETTING IN TOUCH WITH THE EU

In person

All over the European Union there are hundreds of Europe Direct centres. You can find the address of the centre nearest you online (european-union.europa.eu/contact-eu/meet-us_en).

On the phone or in writing

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

— by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),

— at the following standard number: +32 22999696,

— via the following form: european-union.europa.eu/contact-eu/write-us_en.

FINDING INFORMATION ABOUT THE EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website (european-union.europa.eu).

EU publications

You can view or order EU publications at op.europa.eu/en/publications. Multiple copies of free publications can be obtained by contacting Europe Direct or your local documentation centre (european-union.europa.eu/contact-eu/meet-us_en).

EU law and related documents

For access to legal information from the EU, including all EU law since 1951 in all the official language versions, go to EUR-Lex (eur-lex.europa.eu).

Open data from the EU

The portal data.europa.eu provides access to open datasets from the EU institutions, bodies and agencies. These can be downloaded and reused for free, for both commercial and non-commercial purposes. The portal also provides access to a wealth of datasets from European countries.

Publications Office
of the European Union