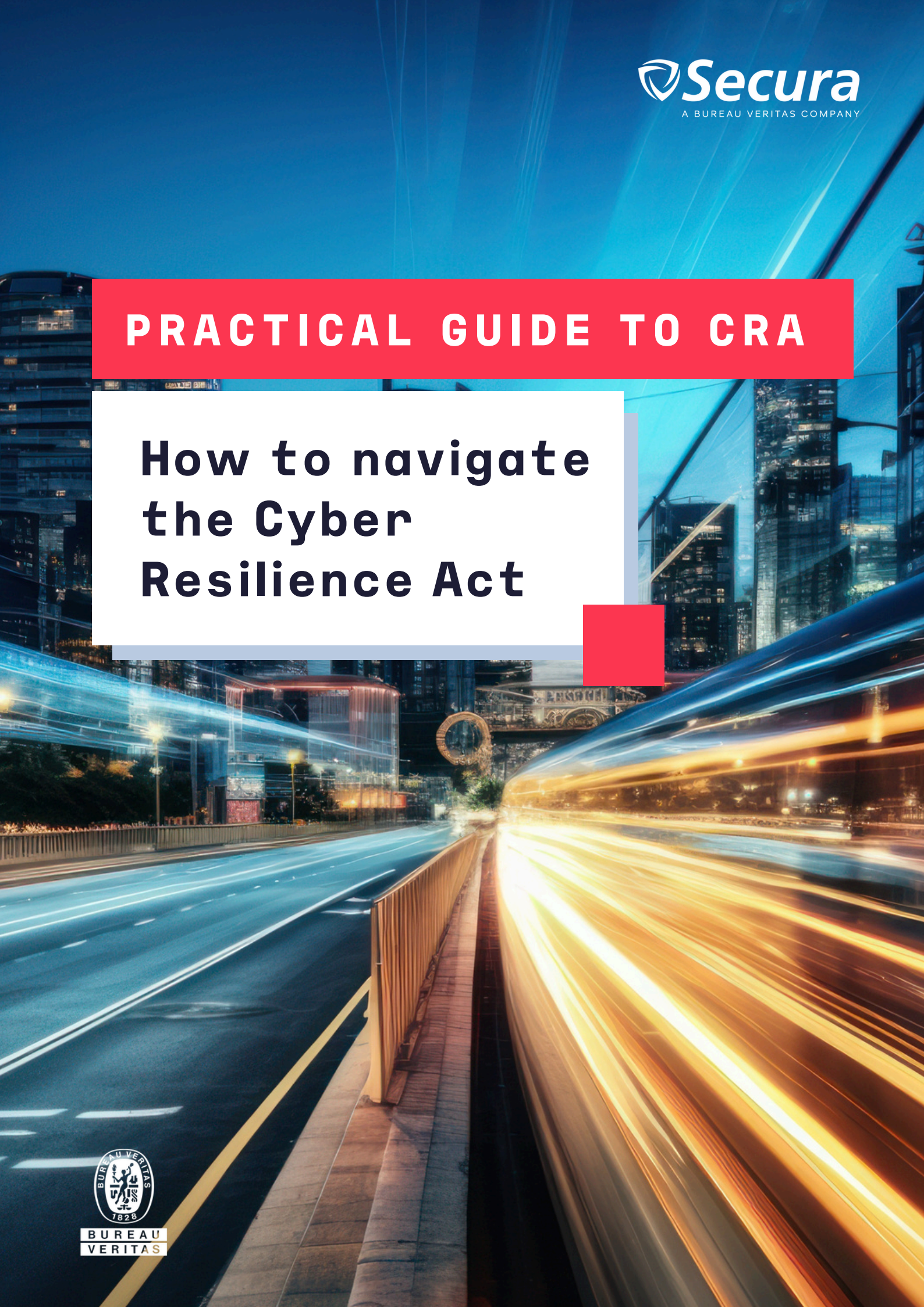
Secura
A BUREAU VERITAS COMPANY

PRACTICAL GUIDE TO CRA

How to navigate the Cyber Resilience Act



BUREAU VERITAS

Contact us

Contact us today for more information on how we can help your organization reach CRA compliance.

 **info@secura.com**

 **+31 (0) 88 888 3100**

 **secura.com**

CONTENTS

TABLE OF CONTENTS

‘Protecting Europe from real and current cyber threats: that is the driving force behind the EU’s Cyber Resilience Act. How will the CRA impact your organization? This document gives you an overview and insights to help you on your way to compliance.’

Razvan Venter
Manager Market Group Product Manufacturers | Secura BV

1. What is CRA and why do we need it?

The **Cyber Resilience Act (CRA)** is a new EU cybersecurity legislation. It is designed to make sure products with digital elements are developed more securely, ultimately protecting consumers all over Europe. It supplements the existing legal framework for the CE mark (EU declaration of conformity) for security properties.

The Cyber Resilience Act introduces mandatory cybersecurity requirements for hardware and software products, throughout their entire life cycle. CRA is aligned with the requirements of the RED Delegated Regulation and it is expected that the latter will be amended or repealed to ensure legal clarity. CRA will complement the NIS2 Directive.

The act was agreed to in **December 2023** and will enter into force in **2024**. Companies will then have 36 months to comply, with one exception: the reporting obligations regarding actively exploited vulnerabilities and incidents will be enforced 21 months after the CRA enters into force.

The Cyber Resilience Act addresses the escalating global cost of cybercrime, fueled by cyber attacks on hardware and software products. Most hardware and software products are currently not covered by any EU legislation regarding their cybersecurity. The current EU legal framework does not address the cybersecurity of non-embedded software. The CRA aims to change this.

2. To which products does CRA apply?

The Cyber Resilience Act covers all products with digital elements which are directly or indirectly, logically, or physically connected to a device or network.

The regulation distinguishes between the majority of products and two special categories that pose a higher cybersecurity risk. The first special category is represented by the **important** products which is further divided into *class I* and *class II*. The second special category is represented by the **critical** products, which pose the highest risk.

The main particularity for the products belonging to the special categories is that they have to undergo stricter conformity assessments. Most products with digital elements will require a form of conformity assessment based on internal control (self-assessment). For the important products with digital elements the following apply:

- Class I: Conformity assessment based on internal control following harmonized standards, common specifications or European cybersecurity certification schemes;
- Class II: The same as for Class I, but it is mandatory that the conformity assessment is involving a third party.

For the conformity assessment of critical products with digital elements, **mandatory compliance to certification schemes such as the EUCC** at level at least “substantial” is required.

IMPORTANT PRODUCTS

CLASS 1:

SIEM SYSTEMS

NETWORK MANAGEMENT SYSTEMS

ROUTERS AND SWITCHES

IDENTITY MANAGEMENT AND ACCESS SOFTWARE

PASSWORD MANAGERS

CLASS 2:

TAMPER RESISTANT MICRO-PROCESSORS

INTRUSION DETECTION AND PREVENTION SYSTEMS

HYPERVISORS AND CONTAINER RUNTIME SYSTEMS

FIREWALLS

TAMPER RESISTANT MICRO-CONTROLLERS

CRITICAL PRODUCTS

HARDWARE SECURITY MODULES (HSM)

SMART METER GATEWAYS WITHIN SMART METERING SYSTEMS

SMARTCARDS

3. What are the main security requirements of the Cyber Resilience Act and what do they mean in practice?

The Cyber Resilience Act has 4 main objectives:

1. Ensure that manufacturers **improve the security of products** with digital elements from the design and development phase and throughout the whole life cycle.
2. Ensure a **coherent cybersecurity framework**, facilitating compliance for hardware and software producers.
3. Enhance the **transparency of security properties** of products with digital elements.
4. Enable businesses and consumers to **use these products securely**.

All requirements of the CRA follow these objectives. The requirements all apply to all types and classes of products. However, the difference between the impact lies in the **conformity assessment.**

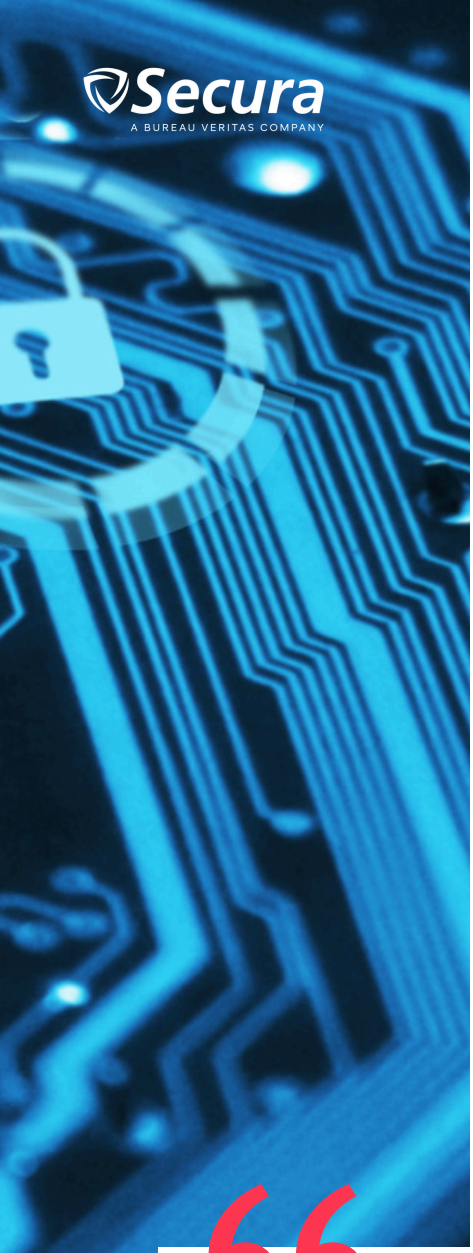
The main requirements regarding cybersecurity properties and vulnerability handling are specified in detail in ANNEX I of the EU proposal text.

The proposal for the Cyber Resilience Act contains 71 articles.

ANNEX I CYBER RESILIENCE ACT

‘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.’

[From the EU proposal text, 2019-2024]



4. How does the CRA relate to other cybersecurity regulations and standards?

The Cyber Resilience Act does not exist in a vacuum. This act will complement the EU **NIS2 Directive**: improving the cybersecurity of products that have digital features will help companies follow the rules of the NIS2 Directive and strengthen the security of the whole supply chain.

The CRA also closely resembles existing cybersecurity standards such as the **ETSI 303 645**, **IEC 62443** and the **European Common Criteria (EUCC)**. Looking at the text of the CRA proposal and at the current landscape of cybersecurity standards, we believe that achieving compliance with the ETSI 303 645, IEC 62443 and/or EUCC will mean you will be close to compliance with the Cyber Resilience Act in the future.

These standards have wide international recognition, as well as very good applicability to the scope of connected products. If you want to be pro-active in pursuing CRA compliance, we advise you to follow these standards.

You can find a detailed mapping of the CRA requirements to the ISO 27001/2, ETSI 303 645, IEC 62443, ISO/IEC 15408 (Common Criteria) in Appendix A. The mapping is based on the **ENISA Cyber Resilience Act Requirements Standards Mapping.**

‘The Cyber Resilience Act marks the first-ever EU-wide legislation of its kind, mandating cybersecurity requirements for both hardware and software products throughout their entire life cycle.’

Raluca Viziteu
Certification Specialist at Secura

5. How we can help you reach compliance with the Cyber Resilience Act

Translating the requirements of the Cyber Resilience Act into practical and appropriate measures requires specific expertise. Secura and Bureau Veritas can help you reach CRA compliance, as we are doing for a number of customers already. We offer the following services:

CRA Presentation

What does the CRA mean for your organization? It takes a lot of time to master the details of this cybersecurity act. You can invite one of our experts to conduct a presentation on this subject. You will gain a thorough understanding of the ins and outs of the CRA. For instance, we can explain the different conformity assessments and which rules apply to your particular product.

Gap Assessment and Certification

How do you determine which measures you need to implement to reach CRA compliance? We can help you with this. We have extensive experience in Gap Assessments and Certification for IEC 62443, ISO 27001/2 and we are a recognized Common Criteria laboratory. Thus, we can also support with Common Criteria/EU CC consultancy and certification.

CRA Implementation Support

After we identify potential gaps between your current security measures and the requirements of the CRA, we can provide consultancy services to solve them and help you become CRA compliant.

The word 'critical' is mentioned 52 times in the CRA text: the regulation prioritizes raising the cybersecurity of products that are vital to society.

Appendix A.
Mapping CRA to existing cybersecurity standards

Security Requirements relating to properties of products with digital elements

	Cyber Resilience Act	Standards	Overall coverage and possible gaps
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	• EN ISO/IEC 27002: 2022 • EN IEC 62443-3- 2:2020 • EN IEC 62443-4- 1:2018 • ETSI EN 303 645 V2.1.1 (2020-06)	The various components of this requirement are covered within major cybersecurity standards. Within the selected standards, the gaps may be summarized 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
2	**On the basis of the cybersecurity risk assessment and where applicable, products with digital elements shall:**		
a	be made available on the market without any known exploitable vulnerabilities	• EN IEC 62443-4- 1:2018 • ETSI EN 303 645 V2.1.1 (2020-06)	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 only vulnerability detection is covered and not the patching of the discovered vulnerabilities, so in general not covering the whole requirement. ETSI EN 303 645 describes only the necessity to deliver products without vulnerabilities.
b	be made available on the market with a secure by default configuration, unless otherwise agreed between manufacturer and business user in relation to a tailor-made product with digital elements, including the possibility to reset the product to its original state	• EN ISO/IEC 27002: 2022 • ETSI EN 303 645 V2.1.1 (2020-06)	Aspects related to product configuration/credentials management 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.

	Cyber Resilience Act	Standards	Overall coverage and possible gaps
c	ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic security updates that are installed within an appropriate timeframe enabled as a default setting, with a clear and easy to use opt-out mechanism, through notification of available updates to users, and the option to temporarily postpone them;	• EN ISO/IEC 27002: 2022 • EN IEC 62443-2- 1:2010 • EN IEC 62443-4- 2:2019 • ETSI EN 303 645 V2.1.1 (2020-06)	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.
d	ensure protection from unauthorized access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible unauthorized access	• EN IEC 62443-4- 2:2019 • ETSI EN 303 645 V2.1.1 (2020-06)	The standards cover the following areas: authentication, identity & access management, and access control. It should be noted that the standards are mainly of generic nature and in most cases do not cover specific mechanisms and services.
e	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, and by using other technical means	• EN IEC 62443-4- 2:2019 • ETSI EN 303 645 V2.1.1 (2020-06)	The 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.
f	protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorized by the user, and report on corruptions	• EN IEC 62443-4- 2:2019 • ETSI EN 303 645 V2.1.1 (2020-06)	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.
g	process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended purpose of the product with digital elements ('minimization of data')	• ETSI EN 303 645 V2.1.1 (2020-06)	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.
h	protect the availability of essential and basic functions, also after an incident, including the resilience and mitigation measures against of denial-of-service attacks	• EN ISO/IEC 27002: 2022 • EN IEC 62443-4- 2:2019 • ETSI EN 303 645 V2.1.1 (2020-06)	Broad scope 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. 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.
i	minimize the negative impact by the products themselves or connected devices on the availability of services provided by other devices or networks	• ETSI EN 303 645 V2.1.1 (2020-06)	Requirement 2(i) 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.

	Cyber Resilience Act	Standards	Overall coverage and possible gaps
j	be designed, developed and produced to limit attack surfaces, including external interfaces	• ISO/IEC 15408-2:2022 • EN IEC 62443-4- 2:2019 • ETSI EN 303 645 V2.1.1 (2020-06)	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 IEC 62443-4-2:2019 is a partial exception to this as it includes concrete requirements although limited to industrial automation and control systems.
k	be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques	• EN ISO/IEC 27002: 2022 • EN ISO/IEC 27001: 2022 • ISO/IEC 15408-2:2022 • EN IEC 62443-3- 2:2020 • ETSI EN 303 645 V2.1.1 (2020-06)	The standards provide a solid foundation in secure system design, secure product development, risk assessment, security evaluation, and security controls. However, some aspects of defense in depth, sandboxing, and certain mitigation techniques might not be explicitly covered by the selected standards.
l	provide security related information by recording and monitoring relevant internal activity, including the access to or modification of data, services or functions, with an opt-out mechanism for the user	• EN ISO/IEC 27002: 2022 • EN IEC 62443-4- 2:2019 • ETSI EN 303 645 V2.1.1 (2020-06)	ISO/IEC 27002:2022 gives a 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.
m	provide the possibility for users to securely and easily remove on a permanent basis all data and settings and, where such data can be transferred to other products or systems, ensure that this is done in a secure manner	• ETSI EN 303 645 V2.1.1 (2020-06)	The standard outlines broad measures for data erasure. It would also benefit from better reference to some explicit GDPR specific best practices to be more effective.

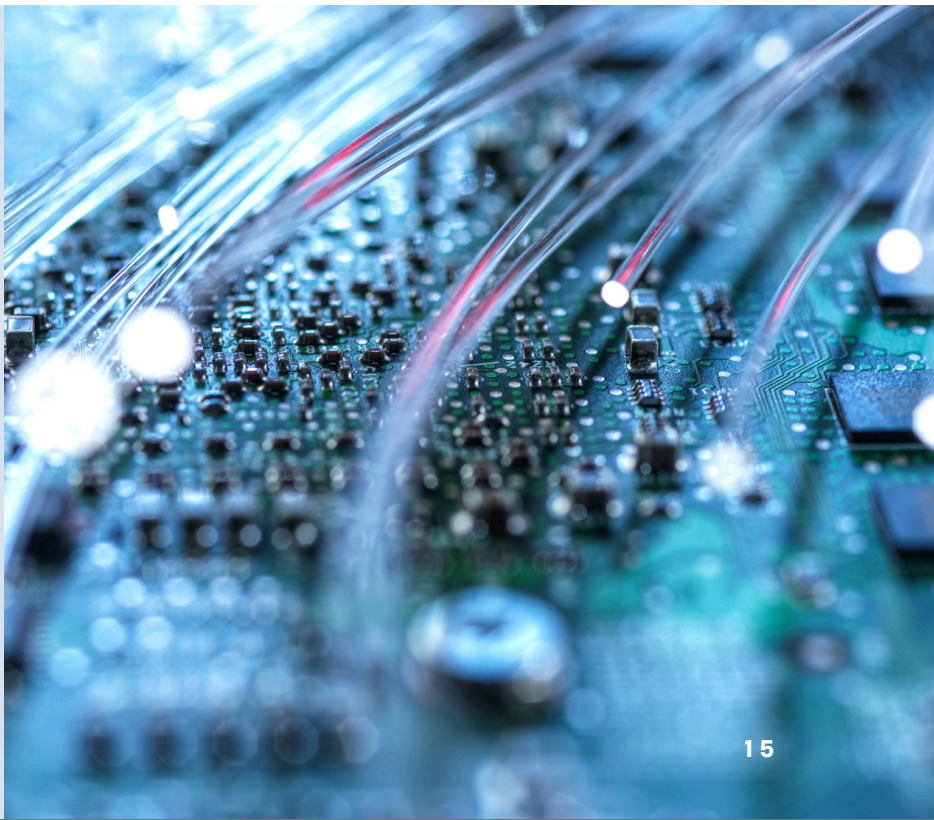
Vulnerability Handling Requirements

	Cyber Resilience Act	Standards	Overall coverage and possible gaps
	Manufacturers of the products with digital elements shall:		
1	identify and document vulnerabilities and components contained in the products with digital elements, 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 products	-	To address the gaps 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. — NTIA's Software Component Transparency Initiative: A U.S. initiative working on standardizing SBOM formats and best practices for software component transparency. — CycloneDX: An SBOM specification designed for application security and supply chain component analysis, offering a lightweight format for describing software components and metadata. — ECSO Supply Chain management and Product Certification Composition — IIoTSBOM is an initiative from LSEC, Flanders Make and KU Leuven COSIC from Belgium to improve cybersecurity for devices. Combining these standards and initiatives can help create a comprehensive approach to managing SBOMs, addressing information security risks in supplier relationships, and improving software supply chain transparency.
2	in relation to the risks posed to the products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates, where technically feasible, new security updates shall be provided separately from functionality updates	• EN ISO/IEC 27002: 2022 • EN ISO/IEC 27001: 2022 • EN IEC 62443-4-1:2018	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.

	Cyber Resilience Act	Standards	Overall coverage and possible gaps
3	apply effective and regular tests and reviews of the security of the product with digital elements	• EN ISO/IEC 27002: 2022 • EN ISO/IEC 27001: 2022	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.
4	once a security update has been made available, share and publicly disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and clear and accessible information helping users to remediate the vulnerabilities; in duly justified cases, where manufacturers consider the security risks of publication to outweigh the security benefits, they may delay making public information regarding a fixed vulnerability until after users have been given the possibility to apply the relevant patch	• EN IEC 62443-4- 1:2018 • ETSI EN 303 645 V2.1.1 (2020-06)	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, NIST National Vulnerability Database (NVD), FIRST Vulnerability Reporting and Data eXchange (VRDX))
5	put in place and enforce a policy on coordinated vulnerability disclosure	• ETSI EN 303 645 V2.1.1 (2020-06)	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.
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	-	To cover this gap, it could be considered the implementation of a combination of standards, initiatives, and collaborate with national CERTs/CSIRTs and ENISA. 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, FIRST PSIRT Services Framework).

	Cyber Resilience Act	Standards	Overall coverage and possible gaps
7	provide for mechanisms to securely distribute updates for products with digital elements to ensure that vulnerabilities are fixed or mitigated in a timely manner and, where applicable for security updates, in an automatic manner	• EN ISO/IEC 27002: 2022 • EN IEC 62443-4-1:2018	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, NIST SP 800-63B, OWASP SSDLC). It may be possible to take a closer look into the Patch Management mechanism suggest in the EUCC. 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.
8	ensure that, where security updates are available to address identified security issues, they are disseminated without delay and, unless otherwise agreed between a manufacturer and a business user in relation to a tailor-made product with digital elements, free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken	• EN ISO/IEC 27002: 2022 • EN IEC 62443-4-1:2018	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.

The Cyber Resilience Act also covers high risk AI-systems



About Bureau Veritas / Secura

Secura is a leading cybersecurity company. We help customers all over Europe to raise their cyber resilience. Our customers range from government and healthcare to finance and industry. We offer technical services, such as vulnerability assessments, penetration testing and red teaming, but also provide audits, forensic services and awareness training.

Secura is a Bureau Veritas company. Bureau Veritas (BV) is a publicly listed company specialized in testing, inspection and certification. BV was founded in 1828, has over 80.000 employees and is active in 140 countries.

Contact us

Contact us today for more information on how we can help your organization reach CRA compliance.

info@secura.com

+31 (0) 88 888 3100

secura.com