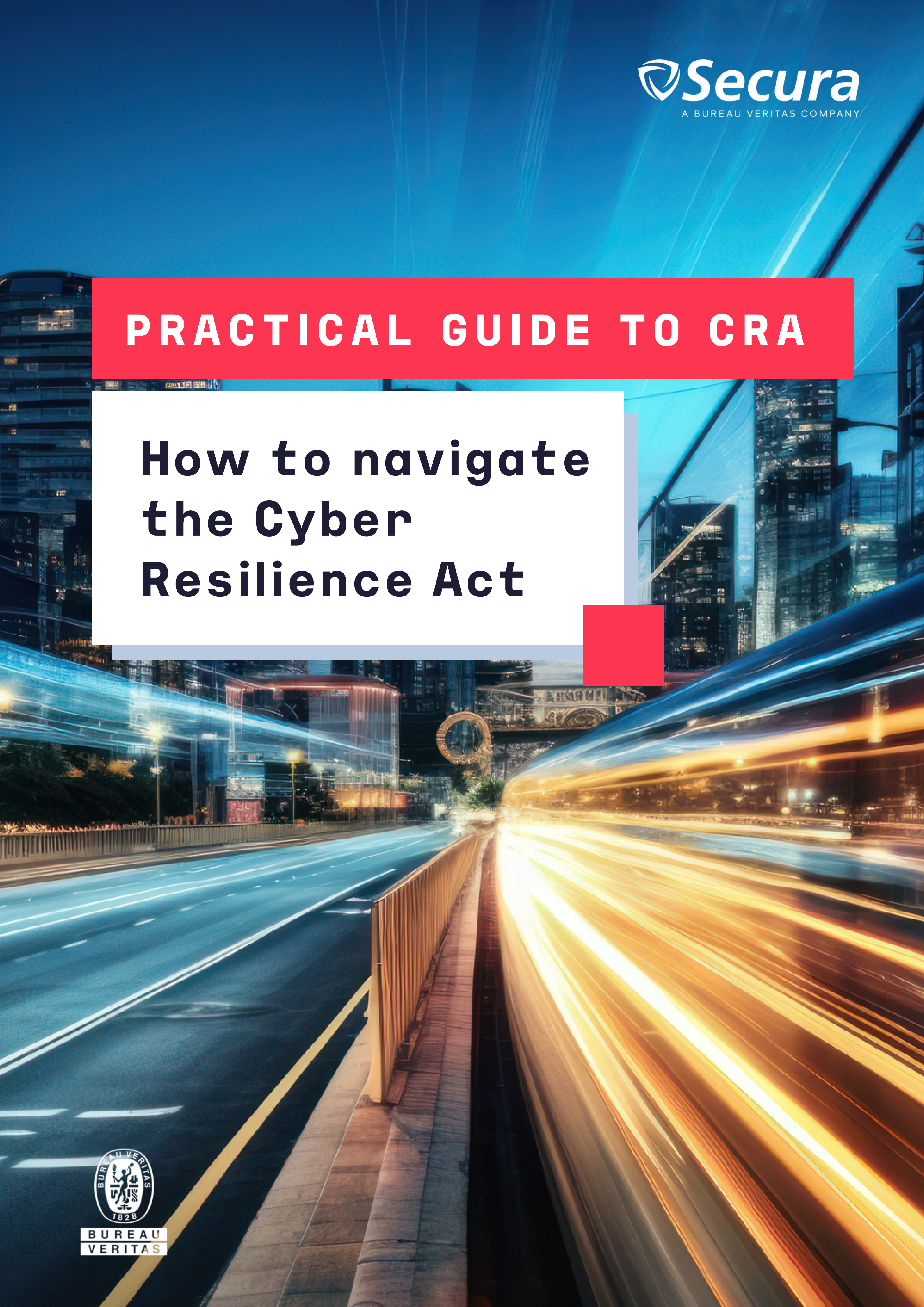
Secura
A BUREAU VERITAS COMPANY



PRACTICAL GUIDE TO CRA

How to navigate the Cyber Resilience Act

BUREAU VERITAS 1828

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

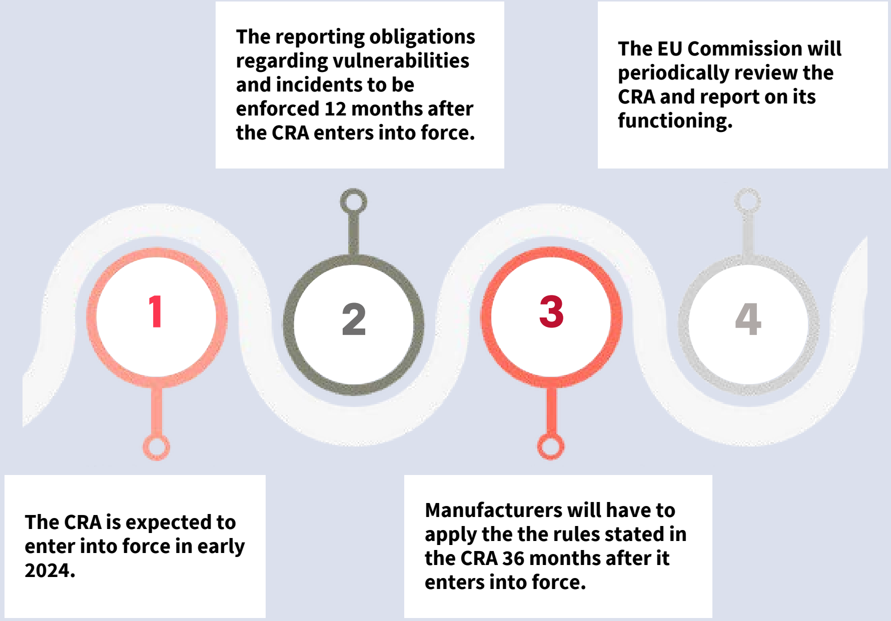
1. What is CRA and why do we need it?

The **Cyber Resilience Act (CRA)** is a new EU cybersecurity legislation. It is designed to make sure any product with digital elements is developed more securely, ultimately protecting consumers all over Europe.

The Cyber Resilience Act introduces mandatory cybersecurity requirements for hardware and software products, throughout their entire life cycle. The CRA will replace the Radio Equipment Directive (RED) and complement the NIS2 Directive. The act was agreed to in **December 2023** and will enter into force at the **beginning of 2024**. Companies will then have 36 months to comply.

The Cyber Resilience Act addresses the escalating global cost of cybercrime, fuelled by cyber attacks on hardware and software products. There are many examples of cyber attacks resulting from insufficient product security, such as the Kaseya VSA supply chain attack in 2021, which abused a vulnerability in Kaseya’s network administration software to attack over one thousand companies.

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.



1 The CRA is expected to enter into force in early 2024.

2 The reporting obligations regarding vulnerabilities and incidents to be enforced 12 months after the CRA enters into force.

3 Manufacturers will have to apply the the rules stated in the CRA 36 months after it enters into force.

4 The EU Commission will periodically review the CRA and report on its functioning.

Companies have 36 months to comply with the Cyber Resilience Act, starting from the beginning of 2024

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 **critical** and **non-critical** products. The critical category is divided into 2 classes, with class 2 being the class expected to run the highest cybersecurity risks.

The cybersecurity risk level is determined by the impact of potential vulnerabilities, the cybersecurity-related functionality of the product and its intended use in sensitive environments such as within an industrial setting. The different categories face different requirements.

CRA does not apply to most medical devices or to aviation or automotive products, as these are covered by existing regulations. The Cyber Resilience Act also does not cover services, such as Software-as-a-Service (SaaS), except for remote data processing solutions associated with a product featuring digital elements. Finally, CRA deliberately excludes free and open-source software that is not developed for profit.

CRITICAL PRODUCTS CLASS 1 includes:

IDENTITY MANAGEMENT AND ACCESS SOFTWARE

PASSWORD MANAGERS

BROWSERS

MICRO-CONTROLLERS

ROUTERS AND MODEMS

SIEM SYSTEMS

NETWORK MANAGEMENT SYSTEMS

CRITICAL PRODUCTS CLASS 2 includes:

OPERATING SYSTEMS FOR SERVERS

FIREWALLS

GENERAL PURPOSE MICRO-POROCESSORS

HARDWARE SECURITY MODULES (HSM)

ROBOT SENSING COMPONENTS

INDUSTRIAL AUTOMATION & CONTROL SYSTEMS (IACS)

INDUSTRIAL IOT DEVICES

```
        <li class="submenu__item"><a href="/sections/movies/" data-metrics-action="click movies">Movies</a></li>
        <li class="submenu__item"><a href="/sections/television/" data-metrics-action="click television">Television</a></li>
        <li class="submenu__item"><a href="/sections/pop-culture/" data-metrics-action="click pop culture">Pop Culture</a></li>
        <li class="submenu__item"><a href="/sections/food/" data-metrics-action="click food">Food</a></li>
        <li class="submenu__item"><a href="/sections/art-design/" data-metrics-action="click art & design">Art &amp; Design</a> </li>
        <li class="submenu__item"><a href="/sections/performing-arts/" data-metrics-action="click performing arts">Performing Arts</a></li>
      </ul>
    </li>
    <li class="menu__item menu__item--music menu__item--has-submenu" data-metrics-hover="toggle music drawer">
      <div class="menu__item-inner">
        <a href="/music/" data-metrics-action="click music">Music</a>
        <button class="menu__toggle-submenu" data-metrics-action="toggle music drawer">Expand/collapse submenu for Music</button>
      </div>
        <ul class="submenu submenu--music"><li class="submenu__item">
 href="https://www.npr.org/series/tiny-desk-concerts/" data-metrics-action="click tiny desk">
  Tiny Desk
a>
li class="submenu__item">
 href="https://www.npr.org/sections/allsongs/" data-metrics-action="click all songs considered">
  All Songs Considered
a>
li class="submenu__item">
```

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

The proposal for the Cyber Resilience Act contains 57 articles.

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**, which is stricter for class II critical products than for class I products.

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

> **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]

CRA | ESSENTIAL CYBERSECURITY REQUIREMENTS

1 **Secure default configuration**
Products need to be delivered with a secure by default configuration, including the possibility to reset the product to its original state. □

2 **Secure access**
Products need to be protected from unauthorized access by control mechanisms: authentication, identity or access management systems. □

3 **Data protection (1)**
Products must protect the confidentiality of stored or transmitted data, for instance by encrypting relevant data at rest or in transit. The encryption methods must be state of the art. □

4 **Data protection (2)**
Companies must protect the integrity of data, personal or other, commands, programs and configuration against manipulation or modification that was not authorized by the user. Corruptions must be reported. □

5 **Minimization of data**
Products must only process data that are relevant. They must keep the data and limited to what is necessary in relation to the use of the product. □

6 **Protection of availability**
Products must protect the availability of essential functions. That means they must be resilient to denial of service attacks. They must also minimize their own impact on the availability of services provided by others. □

7 **Limited attack surface**
Products must be designed, developed and produced in a way that limits attack surfaces, including external interfaces. □

8 **Reducing impact of incidents**
Products must be designed, developed and produced to reduce the impact of an incident. For instance by using appropriate exploitation mitigation mechanisms and techniques. □

9 **Security monitoring**
Products must provide security related information by recording and/or monitoring relevant internal activity. □

10 **Security updates**
Products must be able to address vulnerabilities through security updates, for instance through automatic updates. □

CRA | VULNERABILITY HANDLING REQUIREMENTS

1. **Identifying vulnerabilities**
   Manufacturers are expected to identify and document vulnerabilities and components contained in the product. □

2. **Addressing vulnerabilities**
   If a vulnerability is identified, you are required to address and remediate it without delay, including by providing security updates. □

3. **Regular security testing**
   Manufacturers are expected to apply effective and regular tests and reviews of the security of the product with digital elements. □

4. **Sharing information on vulnerabilities**
   Once a security update has been made available, manufacturers must share information about fixed vulnerabilities with the wider public. You are also expected to create and enforce a policy on vulnerability disclosure, as well as make sure that people can contact you about vulnerabilities. □

5. **Distributing security updates**
   You are expected to provide mechanisms to securely distribute updates for products with digital elements. This is to ensure that exploitable vulnerabilities are fixed or mitigated in a timely manner. Any security patches or updates should be shared quickly and free of charge. □

> **ARTICLE 11** CYBER RESILIENCE ACT
>
> ‘The manufacturer shall, without undue delay and in any event within 24 hours of becoming aware of it, notify to ENISA any actively exploited vulnerability contained in the product with digital elements.’

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 **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 IEC62443 and/or EUCC will mean you will be close to compliance with the Cyber Resilience Act in the future.

These two 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 to the IEC 62443 and EUCC standards in the appendix.

> ‘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

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 for IEC 62443 and are certified for Common Criteria.

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 the IEC 62443 and EUCC standards

Security Requirements relating to properties of products with digital elements

	Cyber Resilience Act	IEC 62443-4-2	EUCC
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	• FR 3: System integrity (SI), CR 3.3: Security functionality verification, CR 3.3 RE(1): Security functionality verification during normal operation	• SAR Family ALC_TAT: Tools and techniques • SAR Family ADV_ARC: Security Architecture • SAR Family ADV_TDS: TOE Design • SAR Family ASE_SPD: Security problem definition
2	Products with digital elements shall be delivered without any known exploitable vulnerabilities	• FR 3: System integrity (SI)	• SAR Class AVA: Vulnerability Assessment, SAR Family AVA_VAN: Vulnerability analysis
3	**On the basis of the risk assessment 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	• FR 3: System integrity (SI) • CR 7.4: Control system recovery and reconstitution	• SAR Family ADV_ARC: Security Architecture • SAR Family ADV_TDS: TOE Design • SFR Family FPT_RCV: Trusted recovery
b	ensure protection from unauthorized access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems	• FR 1: Identification and authentication control (IAC)	• SFR Class FDP: User data protection, SFR Family FDP_SDI: Stored Data Integrity, SFR Family FDP_UIT: Inter-TSF user data integrity transfer protection • SFR Family FCS_COP: Cryptographic operation • SFR Family FMT_MSA Management of security attributes • SFR Family FMT_SMF Specification of Management Functions
c	protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state of the art mechanisms	• FR 4: Data confidentiality (DC)	• SFR Class FCO: Communication • SFR Class FCS: Cryptographic support, SFR Family FCS_COP: Cryptographic operation • SFR Class FDP: User data protection, SFR Family FDP_UCT: Inter-TSF user data confidentiality transfer protection, SFR Family FDP_SDC: Stored data confidentiality
d	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, as well as report on corruptions	• FR 3: System integrity (SI), CR 3.4: Software and information integrity	• SFR Class FDP: User data protection, including SFR Family FDP_SDI: Stored Data Integrity and SFR Family FDP_UIT: Inter-TSF user data integrity transfer protection • SFR Family FCS_COP: Cryptographic operation

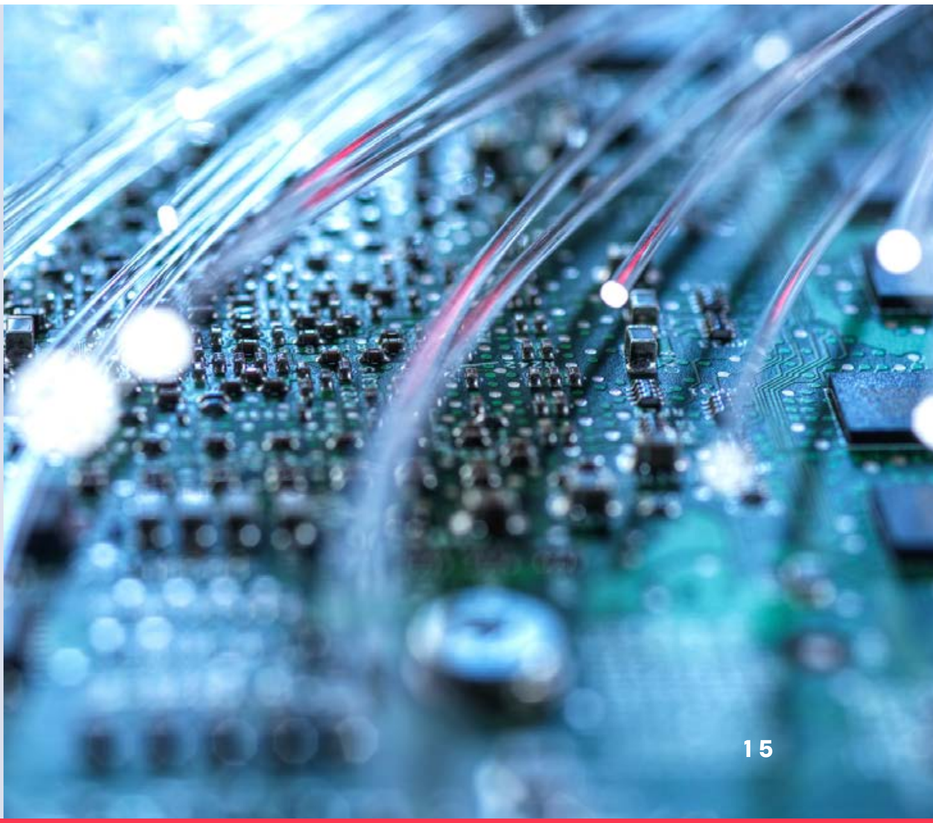
	Cyber Resilience Act	IEC 62443-4-2	EUCC
e	process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended use of the product (‘minimization of data’)	• FR 4: Data confidentiality (DC), CR 4.2: Information persistence	• SFR Class FDP: User data protection, SFR Family FDP_IRC: Information Retention Control
f	protect the availability of essential functions, including the resilience against and mitigation of denial of service attacks	• FR 7: Resource availability (RA)	• SFR Class FRU: Resource utilization, SFR Family FRU_RSA: Resource allocation
g	minimize their own negative impact on the availability of services provided by other devices or networks	• FR 7: Resource availability (RA) • FR 5: Restricted data flow (RDF)	• SFR Class FRU: Resource utilization
h	be designed, developed and produced to limit attack surfaces, including external interfaces	• FR 3: System integrity (SI)	• SAR Family ALC_TAT: Tools and techniques • SAR Family ADV_ARC: Security Architecture • SAR Family ADV_TDS: TOE Design • SAR Family ASE_SPD: Security problem definition • SAR Class AVA: Vulnerability Assessment
i	be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques	• FR 3: System integrity (SI) • FR 6: Timely response to events (TRE)	• SAR Family ALC_TAT: Tools and techniques • SAR Family ADV_ARC: Security Architecture • SAR Family ADV_TDS: TOE Design • SAR Family ASE_SPD: Security problem definition • SAR Class AVA: Vulnerability Assessment
j	provide security related information by recording and/or monitoring relevant internal activity, including the access to or modification of data, services or functions	• FR 6: Timely response to events (TRE) • FR 3: System integrity (SI), CR 3.9: protection of audit information • FR 2: Use Control (UC), CR 2.8: Auditable events	• SFR Class FAU: Security audit, SFR Family FAU_STG: Security audit data storage
k	ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic updates and the notification of available updates to users	• FR 3: System integrity (SI), CR 3.10: Support for updates	• SAR Family ALC_FLR: Flaw Remediation • SAR Class AVA: Vulnerability Assessment, SAR Family AVA_VAN: Vulnerability analysis

Vulnerability Handling Requirements

	Cyber Resilience Act	IEC 62443-4-2	EUCC
	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.	• CR 2.8: Auditable events • CR 7.8: Control system component inventory	• SAR Class AVA: Vulnerability Assessment, SAR Family AVA_VAN: Vulnerability analysis
2	in relation to the risks posed to the products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates.	• FR 6: Timely response to events (TRE)	• SAR Family ALC_FLR: Flaw Remediation • SAR Class AVA: Vulnerability Assessment,SAR Family AVA_VAN: Vulnerability analysis
3	apply effective and regular tests and reviews of the security of the product with digital elements.	• FR 3: System integrity (SI), CR 3.3: Security functionality verification • CR 2.13: Use of physical diagnostic and test interfaces	• SAR Class AVA: Vulnerability Assessment, SAR Family AVA_VAN: Vulnerability analysis
4	once a security update has been made available, 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 information helping users to remediate the vulnerabilities.	• FR 3: System integrity (SI), CR 3.10: Support for updates	• SAR Family ALC_FLR: Flaw Remediation • SAR Class AVA: Vulnerability Assessment,SAR Family AVA_VAN: Vulnerability analysis
5	put in place and enforce a policy on coordinated vulnerability disclosure.	• FR 6: Timely response to events (TRE)	• SAR Family ALC_FLR: Flaw Remediation • SAR Class AVA: Vulnerability Assessment, SAR Family AVA_VAN: Vulnerability analysis

	Cyber Resilience Act	IEC 62443-4-2	EUCC
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.	• FR 6: Timely response to events (TRE)	• SAR Class AVA: Vulnerability Assessment, SAR Family AVA_VAN: Vulnerability analysis, SAR Family AVA_COMP: Composite vulnerability assessment • SAR Family ALC_FLR: Flaw Remediation
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.	• FR 3: System integrity (SI), CR 3.10: Support for updates • FR 6: Timely response to events (TRE)	• SAR Family ALC_FLR: Flaw Remediation • SAR Class AVA: Vulnerability Assessment,SAR Family AVA_VAN: Vulnerability analysis
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.	• FR 3: System integrity (SI), CR 3.10: Support for updates • FR 6: Timely response to events (TRE)	• SAR Family ALC_FLR: Flaw Remediation • SAR Class AVA: Vulnerability Assessment, SAR Family AVA_VAN: Vulnerability analysis

The Cyber Resilience Act also covers high risk AI-systems



Secura

A BUREAU VERITAS COMPANY

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**