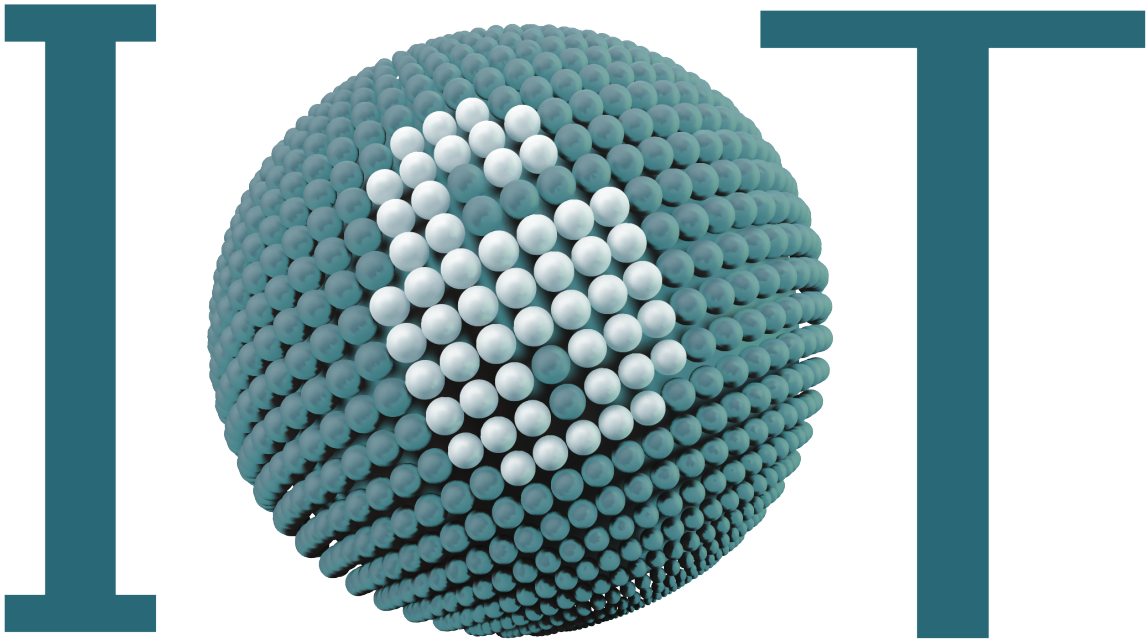

Security Foundation

EUROPEAN UNION CYBER RESILIENCE ACT (EU CRA) EXECUTIVE BRIEF

An IoTSF Regulatory Watch group publication

Cyber Resilience Act (CRA)			
Official Source	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R2847		
Geographic Region	European Union	affected industries	cross-industry
Scope	Products with digital elements		
In brief	The Cyber Resilience Act (CRA) aims to: 1. Increase the level of security of products with digital elements 2. Ensure that users of products with digital elements have sufficient understanding and access to information to select products that have adequate security and to use them securely. For this, it defines essential requirements on the design, development and production of such products, and on associated vulnerability handling processes, as well as rules governing making them available on the market, and for market surveillance and enforcement.		
Consequences	Penalties of up to EUR 15m or 2.5% of global annual revenue		
Baseline Standard	Harmonized standards are currently under development		

EU Cyber Resilience Act

The aim of the European Cyber Resilience Act (CRA) is to improve security of products, and to increase transparency around security to allow customers to take cybersecurity into account when purchasing and operating products. The CRA primarily addresses manufacturers of products with digital elements, but also holds liable importers and distributors. It was initially proposed by the European Commission in September 2022, was signed into law by the EU Council in September 2024 and formally passed into the EU Official Journals (EUOJ) on 20th November 2024. This sets the Entry into Force (EIF) date as 10th December 2024 and the Enforcement date from 11th Dec 2027.

Manufacturers now have 36 months from the EIF date to adapt to the requirements of the Act. An exception to this is vulnerability reporting, for which a 21-month adaptation period is defined. Violations can lead to penalties of up to EUR 15m or 2.5% of the vendor's annual global revenue, whichever is higher.

This IoTSF publication aims to help the reader answer the following questions:

1. Does the CRA apply to me?
2. What do I have to do to achieve and maintain compliance with the Act?
3. How do I do it?
4. What happens if I don't do it?
5. How do I demonstrate conformance to the requirements?
6. Where do I start?

1. Does the CRA apply to me?

The CRA applies to products with digital elements that are placed onto the EU market and have the potential for connection to a device or network [see. Ref. 1 - Article 2]. Products with digital elements that require a CE mark will need to conform to the CRA. Thus, manufacturers, importers, and distributors of IoT products, which by their very nature have digital elements and data connections to devices and/or networks, will need to comply with the CRA unless they are part of specific exempt market sectors that are already regulated or have their own cyber regulations, e.g. medical, automotive equipment, military, aerospace, and national security.

2. What do I have to do to achieve and maintain compliance?

This section mostly relates to the duties of manufacturers of products with digital elements to ensure, a) that their products are secure, and b) that effective vulnerability handling processes are in place to keep them that way. Importers and distributors have an obligation to ensure that these duties have been fulfilled in respect of the products they bring to market.

The CRA defines 'essential cybersecurity requirements' that apply to ALL products with digital elements. However, this does not mean that there is a set of prescriptive rules to follow. The security measures you take to fulfil the requirements need to reflect risk. Furthermore, the evidence that you have to provide by way of assurance depends on the criticality category that the product falls into – more on this later.

Regarding the security properties of products with digital elements, the CRA demands that manufacturers embed security considerations into their design, development and production processes, so as to ensure an appropriate level of cybersecurity based on risk. Thus, it is vital that you conduct a thorough assessment of cybersecurity risk associated with your product at an early stage, and adapt your processes accordingly to incorporate aspects such as:

- Risk Management
- Secure Software Development Lifecycle
- Supply-Chain Management
- Vulnerability Management
- Patch and Update Management

The act lists thirteen security properties that must be addressed based on risk, although not all of them may be applicable to your product. One way to organise your risk assessment, might be to determine which properties are relevant to your product and then to assess and manage the risk that each of these could be violated. Taking this approach should make it easier to provide direct evidence of compliance.

Two of the properties concern management of vulnerabilities: products must have NO known **exploitable** vulnerabilities when released to market, and any exploitable vulnerabilities that are discovered during the lifetime of the product (which should be at least 5 years) must be fixed and security updates made available free of charge, unless an agreement is in place for a tailor-made product. Taken literally, these requirements are not realistic and are at odds with the (sensible) emphasis on risk assessment elsewhere in the CRA. One hopes that they will be interpreted sensibly as referring to known exploitable vulnerabilities adding significantly to cybersecurity risk.

Other properties mandate: a secure by default configuration; the taking of appropriate measures regarding access control, confidentiality, integrity, privacy and availability; the limitation of attack surfaces and of the impact of security incidents; and monitoring and logging of relevant internal activity (although users may opt out of this). In addition, it must be possible securely and easily to remove data, and where relevant, to transfer it to other products and systems.

Most, if not all, of the above will be recognised as merely good security practice, and hopefully, will already be followed by security-aware IoT manufacturers. The difference introduced by the CRA is that manufacturers must provide evidence that they're following such good practice, and that failure to do so may lead to withholding of the right to a CE mark, and to significant financial penalties, as we'll discuss when answering questions 4 and 5, below. It's important, therefore, that manufacturers take advantage of the grace period before enforcement to put in place processes enabling them to demonstrate compliance.

Turning now to vulnerability handling, essential requirements in this category mandate: identification, documentation and remediation of vulnerabilities; regular security reviews and test; secure and timely distribution of software updates and instructions about action to be taken; disclosure of vulnerabilities once they have been fixed; and sharing of information about potential vulnerabilities. Important details include the following:

- To facilitate vulnerability management, you'll be expected to draw up and maintain a SBoM

- If you, a manufacturer, become aware of an actively exploited vulnerability in a product, or of a severe incident having an impact on the security of the product, you must report this within 24 hours both to the CSIRT designated as coordinator in its local member state* and to ENISA. This must be followed within 72 hours by a notification providing additional details on the vulnerability or incident and any mitigating measures deployed. A final report is required within 14 days of a vulnerability mitigation becoming available or within a month of submission of the incident notification.

*The CRA defines rules for determining which Member State is applicable should the manufacturer not have a mail establishment in the EU.

Effective processes for vulnerability disclosure and the maintenance of a Software Bill of Materials (SBoM) are key capabilities that form part of the 'know what you have' and 'know what to do' when something happens aspect of product management. They are critical factors in being able to meet the product vulnerability reporting obligations. Detailed advice on these topics can be found in the IoT Security Foundation publications 'Vulnerability Disclosure Best Practice Guide' [Ref. 2] and the 'Software Bills of Materials for IoT and OT' whitepaper [Ref. 3].

The capability to perform secure updates requires that the product is designed from the outset with this functionality in mind across a secure software supply chain. This is part of the Secure by Design, Secure by Default approach to product design. A mechanism must be in place to maintain the integrity of the update from the point of deployment such that the availability, authenticity, integrity and confidentiality of sensitive or important data or functions in the product is maintained. Amongst other things, this implies the implementation of an authenticated or secure boot mechanism appropriate to the risk level of the product. Lack of such a capability constitutes a severe vulnerability, is also inferred.

Creating a product and providing the relevant supporting business processes and practices, relative to how products are currently brought to and maintained upon the market is a substantial change. This will require a change in mindset and approach to development, with a need to engage with suppliers, product security experts, training organisations and assurance bodies. The IoT Security Foundation and its membership can help you with this.

3. How do I do it?

The same essential security requirements apply to all products. However, different levels of assurance for compliance must be provided depending on the class of product, ranging from self-assessment to product certification by accredited notified bodies. Most products with digital elements will fall under the default classification unless specifically included in a higher class. Those classes requiring stricter levels of conformance are termed **Important** and **Critical** and are discussed in greater detail below.

In general, CRA focusses on principles underlying security but further details on how these principles can be satisfied is expected in additional standards that are still under development. Meanwhile, existing standards can provide useful guidance where their scope applies [see e.g. Ref. 4]. In particular, attaining conformance with EN 18031, ETSI EN 303645, or IEC 62443 is a good starting point.

See below for details on conformance classes and assessment methods.

4. What happens if I don't do it?

Technically, the requirements of the CRA will extend the CE marking, making it mandatory for any product with digital elements to comply with the requirements of the CRA. If you do not comply with the CRA, you cannot apply a CE mark to your product and so cannot sell it in the EU. If a CE mark is applied fraudulently, the product will have to be recalled and will not be allowed to be sold on the EU market. Violations of the CRA will lead to penalties of up to EUR 15m or 2.5% of the vendor's annual global revenue, whichever is higher.

5. How do I demonstrate conformance to the requirements?

All connected devices will have to conform to the terms of the Act. In many cases, the Commission maintains this will be the responsibility of manufacturers who will have to produce a written declaration of conformity (a self-declaration). The Technical Documentation for the product must include an assessment of the security risks and mitigations and any applicable testing undertaken to prove conformity.

There are different certification requirements for certain components/products. For this purpose, products are divided into multiple classes Default, Important and Critical:

Default: Most products with digital elements will fall under default classification unless specifically included in a higher class listed in the Annex III of the regulation.

Important - Class I Includes:

Identity and access management software and hardware incl. authentication and access control incl. biometric readers, Standalone and Embedded Browsers, Password managers, Malicious software detection, Products that use virtual private networks, Network management, configuration, monitoring, and resource management tools, Security information and event management (SIEM) systems, Boot Managers, PKI and Digital Certificate Issuance Software, Operating Systems, Physical and virtual network interfaces, Microcontrollers, Microprocessors, FPGA's and ASIC's with security related features, Smart Home assistants and Smart Home products with security functionalities, Internet connected toys with social interactive features and Personal wearables with health monitoring and/or tracking capability

Important - Class II includes:

Hypervisors and container runtime systems, Firewalls, intrusion detection/prevention systems, Tamper resistant Microcontrollers and Microprocessors

Critical includes:

Hardware device with security boxes, Smart meter gateways and smartcards or similar devices including secure elements.

The following table shows the possible routes to gaining conformity based on device class:

Default	Important Class I	Important Class II	Critical	Assessment type
✅	❌	❌	❌	Basic self-assessment
🆗	✅	❌	❌	Self-assessment to EU Harmonised Standard
🆗	🆗	✅	🆗 *	3rd Party Product Assessment by accredited Notified Body
🆗	🆗	🆗	✅	Certification to EU scheme (if available)

*Note: For products in critical class. If a scheme exists, then certification to the scheme is mandatory. Where no scheme exists a fallback to 3rd Party Product Assessment is allowed.

✅ - Minimum method of assessment
🆗 - Can use this method of assessment
❌ - Cannot use this method of assessment

The Act lays out in some detail the general criteria to be used in judging conformity for the purposes of the assessment. These include that the product SHALL:

- Be designed, developed, and produced with an appropriate level of cybersecurity
- Be delivered without known exploitable vulnerabilities
- Be provided with a secure-by-default configuration, protect against unauthorized access through tools like authentication and identity management
- Protect the confidentiality of data by processing and potentially encrypting relevant data
- Protect the integrity of stored, transmitted, or processed data
- Minimize the collection of data to only process what is adequate and relevant for intended use
- Mitigate denial of essential functions or services
- Reduce the lack of availability of services provided by other devices
- Limit attack surfaces
- Reduce the exploitative effects and impact of a cybersecurity incident with record or monitor relevant security-related information
- Address future vulnerabilities through security updates, preferably automatic ones that notify users

It is also required that in support of the product the company shall:

- Produce a Software Bill of Materials (SBoM), provide security updates, have a vulnerability reporting and management process and perform regular and effective security reviews of the product.

6. Where do I start?

Guidance in support of many of the processes required under the CRA can be found on the IoT Security Foundation website, https://iotsecurityfoundation.org/best-practice-guidelines/ including, Vulnerability Disclosure and Secure Design Best Practice, Supply Chain and SBoM whitepapers plus the IoT Assurance Framework. We recommend that a threat modelling process using a methodology such as the STRIDE model is used throughout the product lifecycle from initial definition through retirement from service. This will help mitigate vulnerabilities entering a product through good 'Secure by Design' practices [Ref. 5,6,7] and helps meet the requirement for cyber security to be taken into account in planning, design, development, production, delivery and maintenance phases [Ref. 8].

The EU Cyber Resilience Act relies on numerous harmonised standards which will aim to clarify details of the requirements. The harmonised standards are however, as yet, unavailable and expect to be released over the next 12-24 months. This leaves a period of time in which developers need to start creating compliant products but are awaiting clarification on what to do or, how to do it. Clearly this poses a problem as product development will be more complex and development cycle times will already be compressed to meet the 36 months transition period. Added to which there is a skills shortage. To this end the IoTSF Security Assurance Framework (https://www.af.iotsf.org) seeks to provide an overarching set of best practices which can be followed. These practices are then mappable against a variety of global regulations and standards which allow developers to follow a standardised set of practices to achieve broad market compliance. Since EU CRA is likely the first of many geographic regulations, the ability for developers to design to a set of best practice methods and map these to end markets will make the design process simpler than trying to chase multiple individual standards.

Members of the IoTSF can access a broad community of knowledgeable security professionals who are able to help and support members achieve a successful product release.

Conclusion

The EU Cyber Resilience Act presents a series of significant changes aimed at making products available on the EU market resilient to cyber-attack and to reduce vulnerabilities created by historically poor security in connected products. It also aims to allow customers to take cybersecurity into account when purchasing and operating products.

The requirements present a challenge to industry due to their broad scope and impact on how companies design, manufacture and maintain a product relative to previous methods.

Organisations should not underestimate the amount of work required to demonstrate compliance. Early engagement in the process and engagement with industry bodies such as the IoT Security Foundation [Ref. 9] and its IoT Security Assurance Framework [Ref. 10] will increase chances of success.

References

1. This document uses the EU Official Journal 2024/2847 regulation of 23 October 2024, version of the EU Cyber Resilience Act as the document of reference https://eur-lex.europa.eu/eli/reg/2024/2847

2. Vulnerability Disclosure Best Practice Guide
    a. https://iotsecurityfoundation.org/wp-content/uploads/2021/09/IoTSF-Vulnerability-Disclosure-Best-Practice-Guidelines-Release-2.0.pdf

3. Software Bills of Materials for IoT and OT whitepaper
    a. https://iotsecurityfoundation.org/wp-content/uploads/2023/02/RELEASE-2022-02-19-IoTSF-SBOM-whitepaper-v1-1-0.pdf

4. Cyber Resilience Act Requirements Standards Mapping, ENISA report ISSN 1831-9424, https://www.enisa.europa.eu/sites/default/files/2024-11/Cyber%20Resilience%20Act%20Requirements%20Standards%20Mapping%20-%20final_with_identifiers_0.pdf

5. Conducting a STRIDE based Threat Analysis
    a. https://www.gov.uk/government/publications/secure-connected-places-playbook-documents/conducting-a-stride-based-threat-analysis

6. Threat Modelling Process
    a. https://owasp.org/www-community/Threat_Modeling_Process

7. Microsoft Threat Modelling Tool
    a. https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats

8. EU Cyber Resilience Act Fact Sheet
    a. https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-factsheet

9. IoT Security Foundation
    a. https://iotsecurityfoundation.org/

10. IoT Security Foundation - Security Assurance Framework
    a. https://iotsecurityfoundation.org/best-practice-guidelines/
    b. https://af.iotsf.org