An Embedded Engineer's Guide to the EU Cyber Resilience Act (CRA)

Introduction

The Cyber Resilience Act (CRA) represents a fundamental shift in the technology policy, moving cybersecurity from a voluntary best practice into a strict legal gatekeeper for the European market. It stipulates that products within the CRA scope must comply with the relevant CRA obligations before being allowed entry into the EU market.

For embedded developers, product managers, and decision makers, the message is clear: CRA readiness should begin now. The regulation introduces obligations across the full product lifecycle, including secure design, vulnerability handling, security updates, incident reporting, technical documentation, and conformity assessment. This guide translates the CRA's requirements into practical engineering and planning considerations. Each chapter explains a key compliance topic and concludes with an action checklist to assist teams in identifying gaps and starting to address them promptly.

Disclaimer: This document provides a subjective interpretation of the relevant regulations and is intended for informational purposes only. It does not constitute legal advice. For specific legal guidance, please consult a qualified professional.

Table of Contents

1. Shift Happens: An Introduction to the EU CRA

The Cyber Resilience Act, formally Regulation (EU) 2024/2847 of the European Parliament and the Council of the European Union, is a regulation that provides a uniform legal framework for cybersecurity and incident reporting requirements when placing products with digital elements on the EU market, as well as during the product's life cycle.

1.1. What Products are Affected by the CRA?

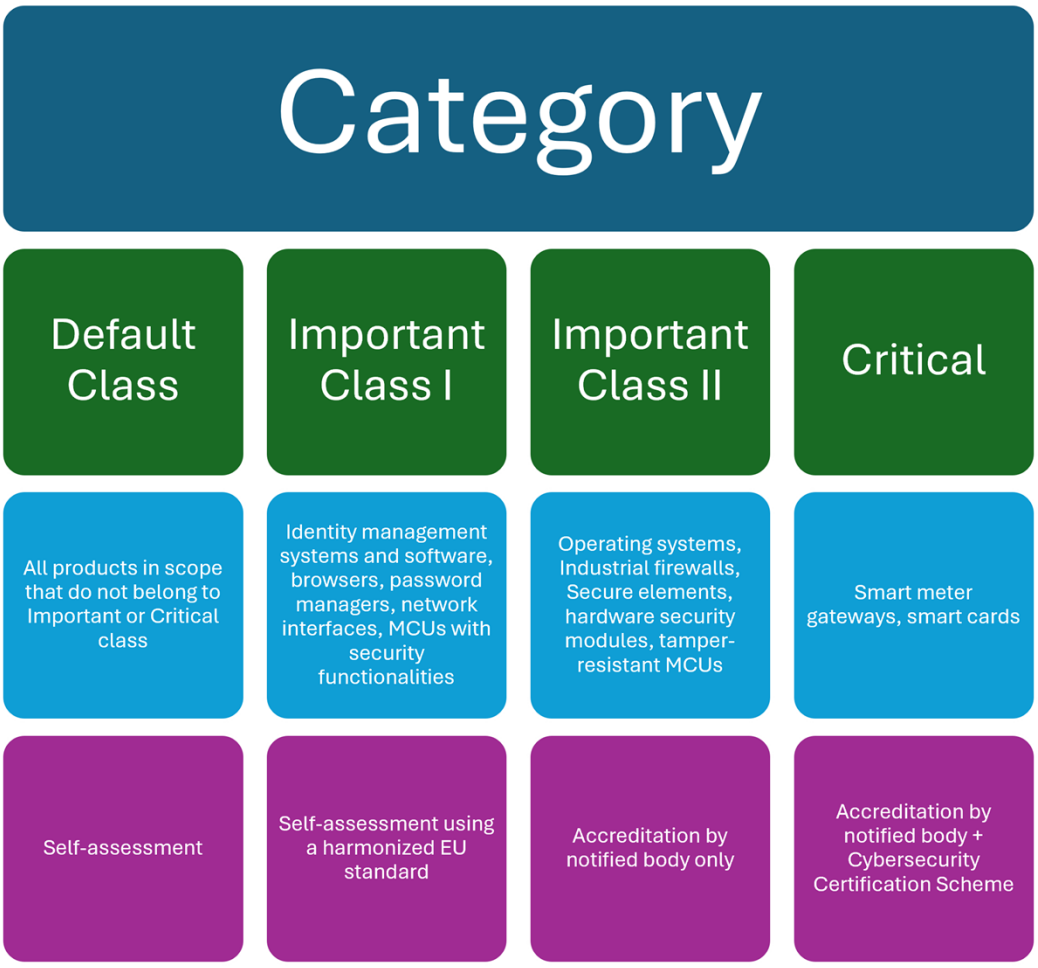
The CRA defines a "product with digital elements" as "*a software or hardware product and its remote data processing solutions".* This also includes individual software or hardware components sold separately. These products are within the scope of the CRA when their intended or foreseeable use includes a direct or indirect data connection to a device or network, whether the connection is logical, physical, or virtual.

Therefore, the CRA covers:

- Standalone software like applications and computer programs
- Hardware with embedded software
- Standalone hardware
- Any combination of hardware and software that are supplied separately but intended to operate together

The CRA also distinguishes between default products and those that are considered important and critical. The product category impacts the conformity assessment path required for the product. These paths range from a simple internal control-based self-assessment all the way up to a cybersecurity certification conducted by a certified third party. The following figure shows a summary of the different product categories. For a comprehensive list of important and critical products, refer to the Annex III of the CRA Specification.

Figure 1-1. CRA Product Classification and Assessment Required



1.2. Who is Required to Comply with the CRA?

Commercial entities placing their products on the European market must comply with the CRA. The term “economic operator” is used as the legal umbrella term to capture entities responsible for bringing a product to the EU market, which includes but is not limited to the following:

- Manufacturers
- Importers
- Distributors
- Authorized representatives, or legal entities who are subject to obligations in relation to making products with digital elements available on the market

1.3. What Does it Mean to Make a Product Available on the European Market?

The CRA distinguishes between placing a product on the market and making a product available.

Placing a product on the market means the first making available of a product with digital elements on the EU market.

Making a product available on the market means supplying a product for distribution or use on the EU market in the course of a commercial activity, whether for payment or free of charge.

Making this distinction is crucial for it determines exactly when an economic operator's legal obligations are triggered. It also starts the clock for the mandatory support period for the products.

The Blue Guide expressly states that placing on the market applies to each individual product, not the product type. Individual units of an existing product family / type placed after new requirements (such as EU CRA) become applicable must comply with those requirements.

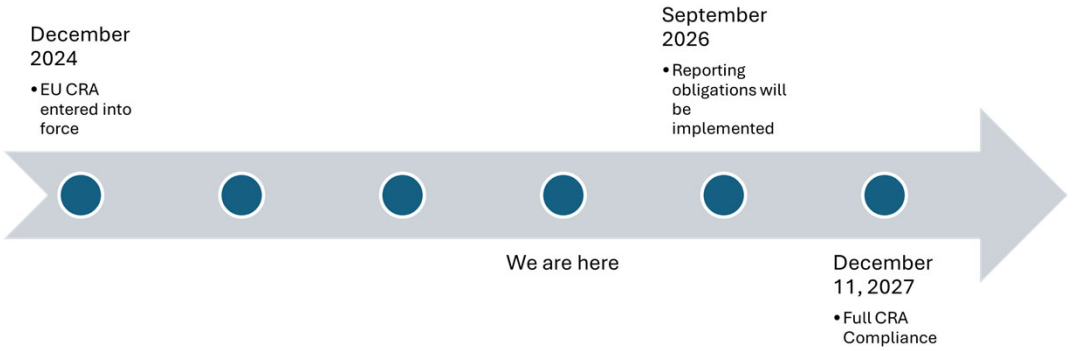
As such, any individual unit first placed on the EU market on or after 11 December 2027 must be fully CRA compliant, even where:

- the same model number has been used for years;
- the hardware and firmware are unchanged;
- most of the design predates the CRA;
- identical units were previously sold in the EU.

1.4. When Does the CRA Take Effect?

The CRA is implemented in phases, with Phase 1 concerning the reporting obligations being implemented first on September 11, 2026, and full CRA compliance to follow in Phase 2 on December 11, 2027. The following figure shows an overview of the timeline for CRA implementation and compliance.

Figure 1-2. CRA Implementation Timeline



1.5. What Do These Requirements Mean for Developers, Engineers, and Decision Makers?

Product Lifetime Responsibility

The CRA mandates manufacturers to take on additional product lifetime responsibilities. They are legally bound to provide security support and patches for at least 5 years (or the expected product-related life cycle, if shorter than 5 years) after the last individual product is made available. The CRA also requires a dedicated Product Security Incident Response Team (PSIRT) to provide timely responses to vulnerabilities and issues discovered in the products. This puts more pressure on engineering resources to rapidly provide software updates and actively monitor any product issues after deployment.

Conformity Assessment and Declaration

Economic operators must perform due diligence to assess and check their products for conformity with the requirements of this legislation. A Declaration of Conformity is required for products to achieve a CE mark, which allows them to be sold on the EU Market. Conducting these assessments and checking the boxes to truthfully declare conformity is a time-consuming and resource-intensive process, especially for products in the important and critical categories.

The Price of Non-Compliance

The CRA makes cybersecurity compliance a legal condition for market entry into the EU. In addition to that, the CRA imposes monetary penalties as high as 15 million euros or up to 2.5% of the worldwide annual turnover revenue. As such, it would be no exaggeration to say that non-compliance can spell economic and financial disaster for economic operators as defined by the CRA.

1.6. What will Happen to Products that were Designed Before the CRA is Fully Implemented but have not Been Placed in the Market?

According to the July 2026 Commission Guidance on the application of the CRA, products designed before the CRA was implemented might be placed on the market under the CRA without redesign, if manufacturers can demonstrate that the products achieve an appropriate level of cybersecurity in the context of their intended or foreseeable use. This can be done through a thorough cybersecurity risk assessment and technical documentation. Similarly, manufacturers must also provide evidence of the vulnerability handling processes laid down in Part II of Annex I.

Regardless of whether products need to be redesigned or not before being placed on the market, manufacturers are still subject to the obligation of ensuring that applicable conformity assessment procedures are carried out, the EU declarations of conformity are drawn up, and the CE marking is affixed to the product.

1.7. Action Checklist

- Identify which products fall within the scope of the CRA.
- For products in scope, categorize them as Default, Important Class I/II, or Critical category.
- Create a plan to conduct a Threat Analysis and Risk Assessment (TARA).
- Check or review any existing security support or software update policy documents.

2. Security by Design: Essential CRA Requirements

2.1. What is the Key Thing to Remember with the CRA Requirements?

The requirements outlined here are meant to guide evaluation and decision-making. Which requirements are to be implemented or not should be determined based on a full understanding of the risks involved.

2.2. What are the CRA Cybersecurity Requirements?

No Known Exploitable Vulnerabilities

Products available on the market should not have any known exploitable vulnerabilities. Chapter I, Article 3 (41) of the CRA defines "*exploitable vulnerability*" as a vulnerability that has the potential to be effectively used by an adversary under practical operational conditions. Any vulnerabilities that can only be exploited in non-practical conditions (i.e. like in a lab or test mode) are not included in this category.

Secure by Default

A product should be in a secure configuration by default and must allow the possibility of resetting the product to its original state, unless otherwise agreed upon by the parties involved.

Automatic, Timely Security Updates

Manufacturers must ensure that all vulnerabilities are addressed through security updates throughout the support period of the product. These updates must be free of charge and, if technically feasible, enabled by default with clear information and opt-out and postponement mechanisms. If updates are not feasible, the justification must be documented implicitly in the compliance documentation.

Protection from Unauthorized Access

Access to the product must be ensured through authentication, identity, or access management mechanisms. Similarly, the firmware running on devices should also be verified and validated.

Data Anonymity and Integrity Protection

Based on the risk assessment and the environment, products must protect the confidentiality, anonymity, and integrity of stored, transmitted, or processed data, personal or otherwise, through appropriate state-of-the-art mechanisms.

Data Minimization

Products must process only data that is adequate, relevant, and necessary for the intended purpose. Access to data and functions should also follow the *principle of least privilege*.

Safe and Secure Recovery from Incidents

The essential and basic functions of a product should remain available after an incident. Similarly, a failure in the product should be isolated and should not impact the product itself or any connected products.

Minimized Attack Surfaces

An attack surface is the total sum of all vulnerabilities, entry points, and pathways—digital, physical, and human—that an unauthorized user can exploit to access or extract data from a system. Minimizing these entry points is an essential first step towards a more secure product.

Data Monitoring

Internal activity relevant to security-related information, such as access to and modification of data, must be monitored, with an opt-out mechanism.

Easy Data Deletion and Migration

Users must be provided with an option to easily, securely, and permanently remove all data and settings they have on the product. Similarly, if the data is to be migrated to other products and systems, this should be performed in a secured way.

2.3. Action Checklist

- Identify the risks associated with the product. Which of these requirements address these risks?
- Assess the product for any known vulnerabilities by searching common vulnerability databases, such as the European Vulnerability Database or the global Common Vulnerabilities and Exposures (CVE) database.
- Check if the default configuration of the device or product is secure.
- Review plans for providing security firmware updates to customers.
- Understand how the product is protected from unauthorized access. If not, how can it be protected?
- Be familiar with how the product handles user data:
  - What data is being gathered by the product, and how much?
  - Does it anonymize the data?
  - What measures are taken to protect the integrity and confidentiality of the data?
  - Can users easily delete, download, or migrate their data?
- Simulate a worst-case attack on the product and identify the impacts of a security fault on the product and on any connected device.

3. Securing the Intangibles: The CRA and Software Products

3.1. Are Software Products In the Scope of the CRA?

Yes. Chapter I, Article 3(4) of the CRA defines software as: “the part of an electronic information system which consists of computer code”. Computer code can mean either machine code, which is the set of instructions directly executed by the processor, or source code, which is the set of instructions written in a programming language and compiled by the computer. As such, all the CRA requirements apply to both standalone software products as well as to software provided as part of the product along with associated hardware.

3.2. Are There Software Products NOT Covered by the CRA?

Yes. Unfinished code shared during the development phase for testing or review is not considered to be placed on the market. Similarly, sample or demonstration code provided as part of any training or tutorials are also out of scope.

3.3. If a Software Product is Made Available Free of Charge or Open Source, Will it Still Fall Under the CRA?

The July 2026 Commission Guidance on CRA application distinguishes between software that is free of charge and software that is open source. Recall the definition of “placing” a product on the market from Chapter 1. The operative term here is “in the course of commercial activity”. Commercial activity is understood as providing goods, whether for payment or free of charge, in a business-related context. If there is a business-related reason why a product is being given free of charge (i.e., promotional purposes, to operate hardware), then it falls within the scope of the CRA.

On the other hand, Free and Open-Source Software (FOSS) is a category of software fulfilling two conditions:

- The software must be made available under a free and open-source license granting the full rights to make the code freely accessible, usable, modifiable, and redistributable.
- The source code must be openly shared on publicly accessible repositories. FOSS products that are not made available for commercial purposes are not under the scope of the CRA.

3.4. I Help Maintain an Open-Source Software Project. Do I have any Responsibilities Toward the CRA?

The CRA defines a new category called an “open-source software steward“. These are organizations that do the work of developing, publishing, maintaining, and sustaining an open-source software project that is used in business contexts. Notable examples that fall into this category are the Linux Foundation, Eclipse Foundation, and the Apache Foundation. These open-source stewards are subject to a lighter touch than manufacturers. While they might not be compelled to provide full technical documentation, they may need to submit other policy or process documentation.

3.5. What if I Use FOSS in a Commercial Product?

Using software that is provided as ‘open source’ and is generally seen as ‘free’ to use is placed on the market with no obligations to the creator (as discussed above). In the context of the CRA, this would be commercializing that software, and therefore the manufacturer inherits responsibility for any vulnerabilities in the product.

3.6. What is an SBOM and How Does it Help with CRA Compliance?

A Software Bill of Materials (SBOM) is a list of all components, libraries, and modules that are included in a software product. Having an SBOM enables teams to track software elements that go into their product, identify vulnerabilities, and prepare contingency plans. Annex I, Part II (1) of the CRA specifically mentions the SBOM as a requirement:

"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."

Annex VII of the CRA also explicitly requires an SBOM to be included in the mandatory technical documentation to be accomplished by the manufacturer:

"Where applicable, **the software bill of materials**, further to a reasoned request from a market surveillance authority provided that it is necessary in order for that authority to be able to check compliance with the essential cybersecurity requirements set out in Annex I."

3.7. Does the CRA Mandate Security Testing to be Performed to Comply with its Requirements?

The CRA does not explicitly require specific tests to be performed, only that manufacturers "*apply effective and regular tests and reviews of the security of the product with digital elements*". However, other requirements, such as only placing products with no known exploitable vulnerabilities, implicitly requires a certain standard in testing products for the requirement to be met. Nevertheless, regular penetration testing, security reviews, and audits are essential in keeping up with the CRA's technical and vulnerability handling requirements.

3.8. Action Checklist

- Ensure that the development process of software products follow secure by design principles or methodologies, such as Secure SDLC.
- Make a list of all the components, libraries, and tools that are being used in the development of a software product. The SBOM starts here.
- Look into automated tools to identify components and generate SBOMs for software products.
- Understand the testing and assessment system in place for software products:
  - Is security adequately tested for software products?
  - Are test results documented and compiled?
  - How often are security reviews and audits carried out by a qualified quality assurance team?

4. In Case of Incident: Vulnerability Handling and Reporting

Phase I of the CRA comes into full effect on September 11, 2026. Phase one requires manufacturers to comply with the full reporting requirements prescribed by the CRA. This section describes what the requirements are and what to do next.

4.1. What are the Requirements for Handling and Disclosing Vulnerabilities to End-users?

Vulnerability Documentation

Manufacturers must identify and document vulnerabilities for at least the top-level dependencies of their product. This document must be in a common and machine-readable format. The SBOM is just part of this documentation. It can be maintained internally or shared with customers if required or appropriate, but the CRA specifically requires it to be available to market surveillance authorities when needed for compliance checks.

Regular Tests and Reviews

Effective and regular security tests and reviews of the product must be conducted and documented properly.

Public Disclosure of Vulnerabilities

Information about potential and fixed vulnerabilities in the products and the third-party components within the product must be disclosed and shared with the public once a security update is available, in addition to notifying the European Union Agency for Cybersecurity (ENISA). This information must allow users to identify the affected product, the impact and severity of the vulnerability, and how to fix or address it. Additionally, information about where to find a list of vulnerabilities and where to report them must also be disseminated clearly and widely.

Coordinated Vulnerability Disclosure Policy

The CRA requires manufacturers to establish and enforce a policy on disclosing incidents and vulnerabilities.

Timely Security Patches Free of Charge

As part of vulnerability handling obligations, manufacturers are responsible for distributing security patches or updates to address identified security issues without delay and free of charge. These updates must be accompanied by advisory messages providing users with relevant information, including the potential action to be taken.

4.2. What Incidents Must be Reported?

Manufacturers must notify relevant authorities, such as the ENISA, through the CRA's Single Reporting Platform (SRP) if they become aware of the following:

- Any actively exploited vulnerability contained in its product
- Any severe incident having an impact on the security of the product

Once the manufacturer becomes aware of the event, the clock starts. "*Becoming aware*" is defined as having a reasonable degree of certainty that a vulnerability is actively exploited or a severe security incident exists. For example, when unusual network activity is detected, it is not necessarily "becoming aware." Once an assessment has confirmed that malicious activity has indeed occurred, the company is now "aware," and the clock officially starts. Manufacturers must have an effective vulnerability-handling and incident-reporting capability. In practice, many organizations implement this through a Product Security Incident Response Team, or PSIRT, but the CRA does not require that every manufacturer use that exact term.

4.3. How Much Time Can Pass Between Reporting an Incident and Filing a Report?

Manufacturers are required to submit early warning notifications containing limited information without undue delay and, in any event, within 24 hours of becoming aware.

Additional information is required as part of the notification to be submitted without undue delay and, in any event, within 72 hours of becoming aware ('72-hour notification'). The complete report needs to be submitted within 14 days after a corrective or mitigating measure is available for actively exploited vulnerabilities, or within one month after the 72-hour notification for severe incidents.

Table 4-1. Reporting Timeline Summary

Time	Action
24 hours after being aware	Submit an early warning notification containing limited information
72 hours after being aware	Complete all information required as part of the notification
14 days after corrective action or mitigating measure	Submit a complete report for actively exploited vulnerability
1 month after the 72-hour notification	Submit a complete report for severe security incident

Users may also need to be informed without undue delay where the vulnerability or incident could adversely affect the security of the product or users' systems.

For additional information on reporting incidents and filing reports, refer to ENISA's SRP FAQ page.

4.4. Action Checklist

- Review security testing procedures in place for development processes.
- Check if a defined and documented internal workflow and policy exists for emergency security reporting and disclosures.
- Establish a public vulnerability disclosure pathway to communicate incidents and issues outside the company.
- Ensure that there are resources for a dedicated PSIRT.
- Determine if vendors have a PSIRT process in place.

5. Compiling for Compliance: CRA Mandated Technical Documentation

5.1. What Role Does Technical Documentation Play in CRA Compliance?

Compliance is proven through documentation and under Chapter III of the CRA. Technical documentation is an integral part defining the conformity of a product with digital elements. Additionally, the CRA sets forth requirements for the documentation to be continuously updated and maintained throughout the product's support period.

Table 5-1. Summary of Conformity Assessment Routes

Product Category	Self-Assessment Allowed?	Notified Body Required?	Details
Default (most products)	Yes (Module A)	No	Manufacturer does everything internally, issues the Declaration of Conformity, and applies the CE mark.
Important – Class I	Yes, but with conditions	Sometimes	Allowed through self-assessment **only if** you fully apply harmonized standards or common specifications. Otherwise, a Notified Body is required.
Important – Class II	No	Yes	Mandatory third-party assessment by a Notified Body.
Critical	No	Yes	Mandatory Notified Body (or European cybersecurity certification scheme).

5.2. What Information Should be Documented to Comply with the CRA?

Annex VII of the CRA is dedicated to the information that should be prepared by manufacturers when they want to declare conformity to the CRA guidelines. Not all of this information must be made available to the public, but having it on hand is good practice in case of market inspection.

Declaration of Conformity

A declaration of conformity (DoC) is a mandatory legal document that an authorized representative of a manufacturer must sign to declare that their products comply with all EU requirements. It is a document that carries a lot of legal weight as it affirms that the manufacturers have undertaken all the necessary assessments and compiled all the documentation to prove compliance.

SBOM

In the case of software products or a combination of hardware and software products, an SBOM is required as a transparency measure, ensuring that these products and their components are carefully vetted and assessed for vulnerabilities.

General Product Description

Manufacturers shall provide a description of the product, including its intended and foreseeable purpose, compliant versions, photos or illustration of the product's external features and internal layout, and instructions for the users.

Product System Architecture

Drawings and schematics of the system architecture explain how hardware and software components build on or feed into each other and integrate into the overall processing.

Vulnerability Handling Process

Manufacturers must provide information on the vulnerability handling processes put in place to mitigate risks and address reported threats. Implementing a coordinated vulnerability disclosure

policy, providing contact details for reporting incidents and vulnerabilities, and establishing mechanisms for the secure distribution of updates fulfill this requirement.

Threat Analysis and Risk Assessment

An assessment of the cybersecurity risks affecting the product, and the essential cybersecurity requirements applicable to the product, must be maintained and documented by the manufacturer.

Support Period Rationale

Relevant information detailing and justifying the support period set by the manufacturer, during which vulnerabilities will be handled effectively, should be documented and maintained.

Applied Standards

In the case where a product also complies with other standards (i.e., ISO21434, IEC62443, EN303-645), common specifications, or cybersecurity schemes, this must also be disclosed and documented.

Test Conformity Reports

Reports of tests carried out to verify that the product conforms to the CRA requirements must be filed and kept for posterity to affirm that due diligence has been done in ensuring that the product is secure.

5.3. Should all the CRA Documentation be Made Available to the Public?

No. Some of the documentation is meant to be kept internally until the manufacturer is required to produce it as evidence of compliance. The following table shows a handy guide to which documents should be kept internally and which should be made available to customers.

Table 5-2. Documentation Guide

Documents to Keep Internally	Documents to Give to Customers
Copy of the EU Declaration of Conformity	EU Declaration of Conformity
Product System Architecture	General Product Description
Threat Assessment and Risk Analysis, Vulnerability Report	Vulnerability Handling Process, Procedures, and Policies
SBOM	SBOM (optional or as stipulated in the contract)
Test Reports	–
Vulnerability Handling Process, Procedures, and Policies	–
Applied Standards	–
Support Period Rationale	–

5.4. Action Checklist

- Review the list of collateral, documentation, and guides being released for each product.
- Identify which documents are missing based on the requirements and determine which existing documents can be improved or modified to satisfy the requirements.
- Create a central repository for "Proof of Compliance" for each product and each version of a product.
- Develop processes that ensure CRA-required documentation is included as part of the final package of a product.
- In case of any informal or verbal-only policies regarding security, formalize them as policy and document them.

6. Bolt On or Build In: The Case for Microchip Security

The CRA essentially makes "security-by-design" a requirement for access to the EU market. Ideally, building in security by integrating secure microcontrollers into a design is the most robust and cost-effective path to compliance to satisfy the CRA requirements. However, for legacy devices and designs, it is completely possible to augment or "bolt on" security using software workarounds and additional hardware. Microchip provides solutions for every scenario, every complexity, and every engineer.

6.1. I Want to Keep my Current Design and Parts. Is it Possible to “Bolt On” Compliance?

Yes. The feasibility of retrofitting an existing design for CRA compliance depends on these factors:

- The risks surrounding the product.
- The capacity available in the product.
- The security use case being implemented.

In the case where all factors favor retrofitting, Microchip can support multiple approaches toward compliance.

For a more hardware-based approach, integrating a secure element into the design, such as Microchip’s CryptoAuthentication™ or Hardware Root of Trust (HRoT) chips paired with Microchip's Secure Bootloaders and Firmware Update Protocols, can secure the design better with minimal rework. For additional information on using these tools and products, visit the Microchip Security Products site, and the Secure MDFU Workflow documentation.

6.2. I am Starting a New Design. How Would Using Secure MCUs Make CRA Compliance Easier?

Supporting Compliance Through Hardware Security

A secure MCU handles the heavy lifting of the CRA’s technical requirements natively. Instead of writing many lines of software to protect keys or verify signatures, hardware blocks can be utilized.

- **Hardware-Accelerated Crypto**: Whether it is an on-chip secure element as seen on the PIC32CM LS60 and PIC32CX SG60/61, or a Hardware Security Module (HSM) peripheral found on the PIC32CK SG00/01 and PIC32CZ CA9x families, Microchip products integrate dedicated hardware to power cryptographic operations that are essential in meeting multiple CRA requirements, such as encryption and authentication, without stalling the main application.
- **Isolated Execution Environments**: Easily satisfy "separation of concerns" by running sensitive code (such as key management) in a Trusted Execution Environment (TEE). Microchip’s Arm® Cortex® M23 and M33 products, such as the PIC32CM LS60, PIC32CM SG00, and the PIC32CK SG00, support Arm TrustZone® which separates the application space into secure and non-secure areas for the secure execution of firmware. The TrustRAM (TRAM) peripheral further secures sensitive data and operations by enabling users to perform data persistence routines to recover data even after memory wipes or to initiate a full erasure of data once tampering is detected.

Lowering Total Cost of Ownership (TCO)

While a secure MCU may have a higher unit price, it significantly reduces engineering hours in the long run:

- **Reduced Audit Risk**: Certified or standards-aligned components simplify the evidence needed for a product-level conformity assessment. Particularly for products that fall under the Default and Important Class I categories, which will follow a self-assessment compliance regiment, having components that are already adhere to known harmonized standards reduces the burden on the manufacturer to compile evidence of compliance.

- **Simplified SBOMs**: By using integrated hardware features, the number of external software libraries (and their associated CVE risks) that need to be tracked is reduced.

Future-Proofing for the 5-Year Support Window

- The CRA requires support products for at least five years after the last individual product is placed in the market. Software-only security fades as new exploits are discovered. Hardware-based security, such as TrustRAM and Anti-Tamper modules, provides a permanent foundation that does not degrade over time.

6.3. What Features do Microchip's Secure MCUs Have That Can Help Fulfill the CRA Essential Requirements?

The following table shows how the security features offered by each Secure MCU family correspond to the particular security operations that address the requirements put forth by the CRA.

Table 6-1. Mapping Secure MCU Family Features to Common Security Operations

CRA Requirement	Device Family					
	PIC32CM SG00	PIC32CM LS60	SAM L11	PIC32CK SG00/01	PIC32CX SG41/60/61	PIC32CZ CA9x
Secure Boot	✓ Secure Boot using HSM-Lite	✓Software solution verified by the ECC608 Secure Element	✓Software solution	✓Secure Boot using HSM	✓Immutable Secure Boot (1)	✓Secure Boot using HSM
Secure Firmware Updates	✓Software solution	✓Software solution	✓Software solution	✓Secure Update supported by HSM	✓Software solution with OTA update support (2)	✓Secure Update supported by HSM
Secure Memory Storage	✓TrustZone ✓Trust RAM ✓ Key wrapping using the Physically Unclonable Function (PUF)	✓TrustZone ✓Integrated ECC608 for secure key storage	✓TrustZone ✓TrustRAM	✓TrustRAM ✓Secure Flash ✓TrustZone	—	✓TrustRAM ✓ Secure Enclave
Cryptography Support	✓Cryptoaccelerators in HSM-Lite	✓Integrated ECC608 Secure Element	✓Cryptoaccelerators	✓Cryptoaccelerators in dedicated M0+ HSM Core	✓Cryptoaccelerators in optional HSM in package	✓Cryptoaccelerators in dedicated M0+ HSM Core
Random Number Generation	✓TRNG in HSM-Lite	✓ TRNG in ECC608 Secure Element	✓Dedicated TRNG peripheral	✓ TRNG in HSM	✓TRNG	✓TRNG in HSM
Tamper Resistance	✓Anti-Tamper Module ✓RTC with Anti-tampering monitoring ✓ Zeroization of TrustRAM	✓Up to 16 Tampering detection pins	✓Up to 4 Tampering detection pins ✓ Zeroization of TrustRAM	✓ Tamper inputs managed by HSM ✓ Zeroization of TrustRAM	✓Up to 5 Tampering detection pins	✓Tamper inputs managed by HSM ✓ Zeroization of TrustRAM

Notes:

1. Immutable/secure boot not available for PIC32CXSG60.
2. Specific software solution available for PIC32CXSG41 available on TPDS. More information can be found at this link: https://www.youtube.com/watch?v=-2g0i0rDAhM.

6.4. Action Checklist

- Based on the risk assessment and the position of the product in its design and life cycle, decide whether the risks allow “bolting on” security features or if a more in-depth security solution must be “built in” and integrated.
- Identify the CRA requirements applicable to the product or design.
- Determine which security implementations will be executed to accomplish the CRA requirements.
- Choose the correct hardware or software solution that has the features to power the security implementations for the product or design.
- For additional information or any questions, contact a local Microchip Field Applications Engineer or Sales Personnel.

7. Useful Links

The official **CRA specification** is **Regulation (EU) 2024/2847** of the European Parliament and of the Council of the 23 of October on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act).

Primary Official Source (Free Access)

- **EUR-Lex (European Union Official Legal Database)**: The authoritative and most reliable place to obtain the full, up-to-date text:
  - **HTML Version**: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng
  - **PDF Version**: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32024R2847

Additional Official Resources

- **European Commission Summary Page**: Contains quick links to the legal text and explanatory materials: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act
- **Standardization Request M/606**: For harmonized standards that support conformity with the CRA essential requirements:
  - Available through the Commission's Documents Register: https://ec.europa.eu/transparency/documents-register/detail?ref=C(2025)618&lang=en
    Harmonized standards are still under development by CEN, CENELEC, and ETSI; they are not yet published in the Official Journal.
- **European Union Agency for Cybersecurity (ENISA)**: For details regarding the Single Reporting Platform (SRP) for CRA and additional details on reporting incidents and filing reports:
  - **ENISA Homepage**: www.enisa.europa.eu/
  - **SRP FAQs**: www.enisa.europa.eu/topics/product-security-and-certification/single-reporting-platform-srp

8. Revision History

Revision A - 08/2026

Initial release of the document.

Microchip Information

Trademarks

The “Microchip” name and logo, the “M” logo, and other names, logos, and brands are registered and unregistered trademarks of Microchip Technology Incorporated or its affiliates and/or subsidiaries in the United States and/or other countries (“Microchip Trademarks”). Information regarding Microchip Trademarks can be found at https://www.microchip.com/en-us/about/legal-information/microchip-trademarks.

Legal Notice

This publication and the information herein may be used only with Microchip products, including to design, test, and integrate Microchip products with your application. Use of this information in any other manner violates these terms. Information regarding device applications is provided only for your convenience and may be superseded by updates. It is your responsibility to ensure that your application meets with your specifications. Contact your local Microchip sales office for additional support or, obtain additional support at www.microchip.com/en-us/support/design-help/client-support-services.

THIS INFORMATION IS PROVIDED BY MICROCHIP “AS IS”. MICROCHIP MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WHETHER EXPRESS OR IMPLIED, WRITTEN OR ORAL, STATUTORY OR OTHERWISE, RELATED TO THE INFORMATION INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE, OR WARRANTIES RELATED TO ITS CONDITION, QUALITY, OR PERFORMANCE.

IN NO EVENT WILL MICROCHIP BE LIABLE FOR ANY INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, OR CONSEQUENTIAL LOSS, DAMAGE, COST, OR EXPENSE OF ANY KIND WHATSOEVER RELATED TO THE INFORMATION OR ITS USE, HOWEVER CAUSED, EVEN IF MICROCHIP HAS BEEN ADVISED OF THE POSSIBILITY OR THE DAMAGES ARE FORESEEABLE. TO THE FULLEST EXTENT ALLOWED BY LAW, MICROCHIP’S TOTAL LIABILITY ON ALL CLAIMS IN ANY WAY RELATED TO THE INFORMATION OR ITS USE WILL NOT EXCEED THE AMOUNT OF FEES, IF ANY, THAT YOU HAVE PAID DIRECTLY TO MICROCHIP FOR THE INFORMATION.

Use of Microchip devices in life support and/or safety applications is entirely at the buyer’s risk, and the buyer agrees to defend, indemnify and hold harmless Microchip from any and all damages, claims, suits, or expenses resulting from such use. No licenses are conveyed, implicitly or otherwise, under any Microchip intellectual property rights unless otherwise stated.

Microchip Devices Code Protection Feature

Note the following details of the code protection feature on Microchip products:

- Microchip products meet the specifications contained in their particular Microchip Data Sheet.
- Microchip believes that its family of products is secure when used in the intended manner, within operating specifications, and under normal conditions.
- Microchip values and aggressively protects its intellectual property rights. Attempts to breach the code protection features of Microchip products are strictly prohibited and may violate the Digital Millennium Copyright Act.
- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of its code. Code protection does not mean that we are guaranteeing the product is “unbreakable”. Code protection is constantly evolving. Microchip is committed to continuously improving the code protection features of our products.