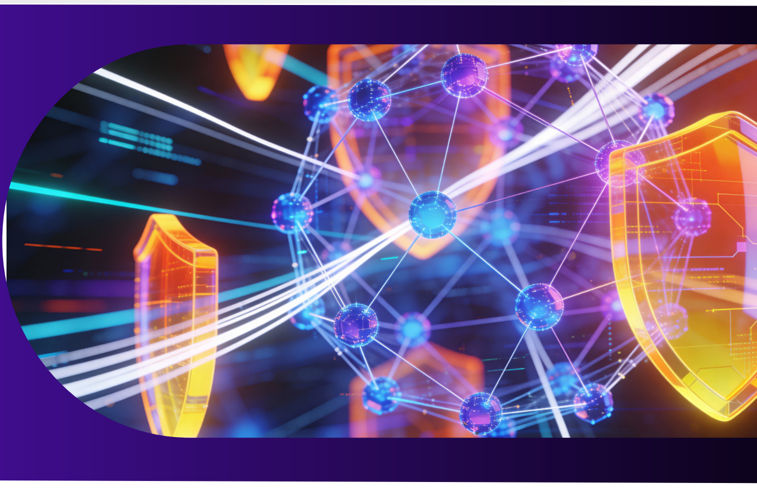
WHITE PAPER

Preparing For The EU Cyber Resilience Act (CRA) with Linaro



Introduction

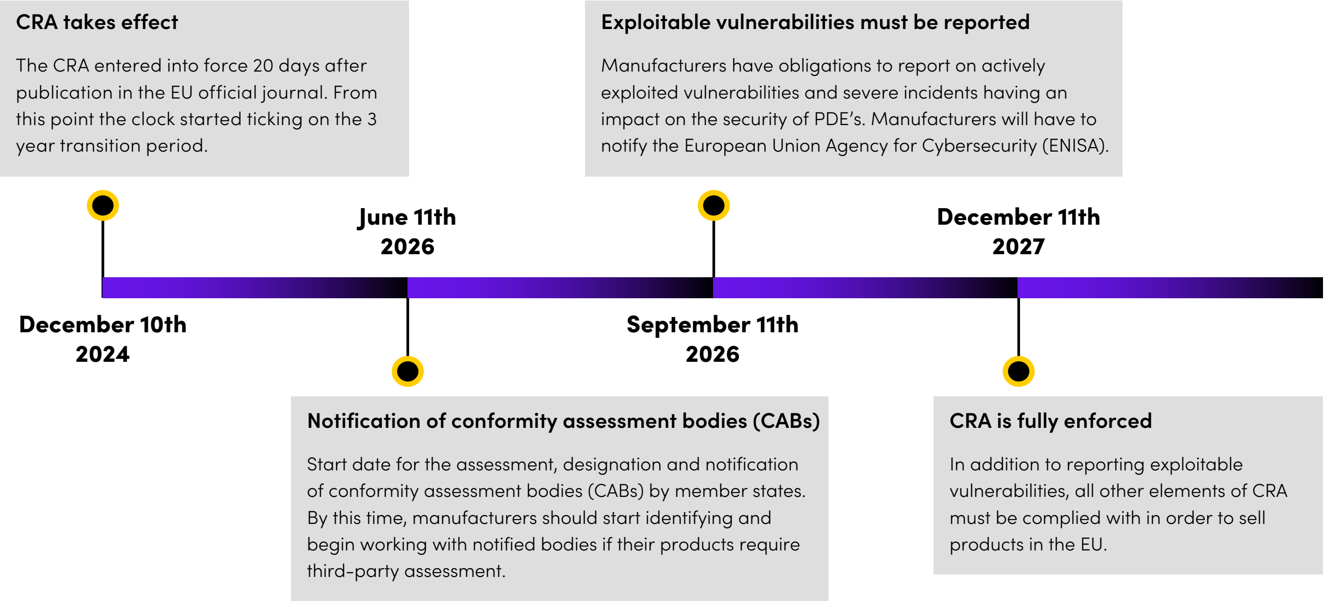
Time is running out for connected device manufacturers. The European Union's new Cyber Resilience Act (CRA) regulation entered into force at the end of 2024, giving manufacturers three years to comply. After that, non-compliant devices may be banned from sale in the EU.

The CRA sets higher cybersecurity standards for almost all products with digital elements sold in Europe. The regulation was created because too many products had inadequate security and slow update cycles, with limited support periods. Now, cybersecurity is a legal requirement to enter the EU market, requiring manufacturers to build in security from the start and maintain it throughout the product's lifecycle.

This paper explains the key points of the CRA, including its requirements, timeline, and scope. We outline how manufacturers can prepare for these changes and how Linaro can help with continuous compliance. By the end of this paper, you will understand what the CRA requires, what's at stake, and how to get ready.

CRA Timeline: When do manufacturers need to act? (Hint: Now)

The CRA will be fully enforced in late 2027, but the transition period has already begun, and some requirements will take effect much sooner.



December 10th 2024

CRA takes effect

The CRA entered into force 20 days after publication in the EU official journal. From this point the clock started ticking on the 3 year transition period.

June 11th 2026

Notification of conformity assessment bodies (CABs)

Start date for the assessment, designation and notification of conformity assessment bodies (CABs) by member states. By this time, manufacturers should start identifying and begin working with notified bodies if their products require third-party assessment.

September 11th 2026

Exploitable vulnerabilities must be reported

Manufacturers have obligations to report on actively exploited vulnerabilities and severe incidents having an impact on the security of PDE's. Manufacturers will have to notify the European Union Agency for Cybersecurity (ENISA).

December 11th 2027

CRA is fully enforced

In addition to reporting exploitable vulnerabilities, all other elements of CRA must be complied with in order to sell products in the EU.

The regulation entered into force on 10 December 2024, starting a three-year transition period. Products can still be sold during this time, but manufacturers should use it to set up security, vulnerability management, and compliance processes.

By **June 11 2026,** conformity assessment bodies (CABs) will start being formally notified. Manufacturers whose products require third-party assessment should already start engaging with suitable assessment partners by this point, rather than treating it as the start of their compliance journey.

Starting **September 11 2026,** manufacturers must report actively exploited vulnerabilities and severe security incidents to the European Union Agency for Cybersecurity (ENISA) and the relevant Member State authority. This requirement takes effect before full enforcement, so manufacturers must have monitoring and incident-response processes in place before the 2027 deadline.

Finally, on **December 11 2027,** the CRA will be fully enforced. From this point onward, all applicable requirements must be met to sell products in the EU, including products that have been on the market for many years.

The key takeaway is that, even though full enforcement is at the end of 2027, manufacturers should start preparing much earlier.

Scope of the CRA: Does it apply to your product?

Before looking at the CRA's detailed requirements, it's important to check if the regulation applies to your product and how it is classified.

In general, the CRA covers all **products with digital elements (PDEs)** sold in the EU, with a few exceptions. A product with digital elements is broadly defined as **hardware or software that connects directly or indirectly to a device or network.** This includes most modern connected products.

The CRA groups PDEs into different risk categories based on cybersecurity risk. These categories affect how compliance is checked and whether third-party involvement is needed.

As part of determining the category a product falls into, it's crucial to first determine the **core functionalities** of the product. This is critical, since a product as a whole can have elements that form **part** of a product, which may in part match the technical description set out in one of the **important categories.** However, if the element matching the technical description is not considered core functionality provided to an end user, then it does not automatically classify the product as a whole in an important category. As a concrete example, if the product were a mobile phone with elements that match **Class I** technical descriptions, such as "password managers" and "operating systems", but these elements were not considered core functionality, i.e. a mobile phone has an operating system but is not the core function provided to a user by the manufacturer, then the mobile phone would typically be considered in the **default category** (unless other core functions were meeting the technical description of the important category).

Manufacturers' products will fall into one of these categories:

Default / Non-Critical / Non-Important products

This category generally includes products with limited cybersecurity impact, such as:

- Games and photo editing software
- Consumer or IoT products without security-related functionality

Manufacturers can self-assess products in this category, taking full responsibility and following the internal control procedure set out in Module A of Decision No 768/2008/EC.

Important Products (Class I)

Class I products include devices and software with security-related functionality, for example:

- Identity management systems and privileged access management software and hardware, including authentication and access control readers
- Standalone and embedded browsers
- Password managers
- Software that searches for, removes or quarantines malicious software
- VPN software
- Network management systems
- Security information and event management (SIEM) systems
- Boot managers
- Public key infrastructure (PKI) and digital certificate issuance software
- Physical and virtual network interfaces
- Operating systems
- Routers, modems, and switches that are intended for internet connectivity
- Microcontrollers, Microprocessors, ASICs and FPGAs with security-related functionalities
- Smart home general-purpose virtual assistants
- Smart home products with security-related functionalities, including smart door locks, security cameras, baby monitoring systems, and alarm systems
- Internet-connected toys that have social interactive features, e.g. speech, video recording, and location tracking
- Personal wearable products that have health monitoring tracking features

Manufacturers can still self-assess these products **if** they use recognised harmonised standards, common specifications, or European cybersecurity certification schemes identified by the European Commission. Harmonised standards are European standards developed by CEN (European Committee for Standardisation), CENELEC (European Committee for Electrotechnical Standardisation), or ETSI (European Telecommunications Standards Institute) at the request of the European Commission.

Harmonised standards fall into two groups. Horizontal standards are product-agnostic and provide a general approach to cybersecurity across sectors. Vertical standards are product-specific and address the unique cybersecurity needs of different digital product types. If these standards are not used, a third-party conformity assessment is required.

Important products (Class II)

Class II products are higher risk and include:

- Tamper-resistant microcontrollers & microprocessors
- Firewalls, Intrusion detection and prevention systems
- Hypervisors and container runtime systems that support virtualised execution of operating systems and similar environments

Self-assessment is not allowed for this category. An external third party must assess these products.

Critical products

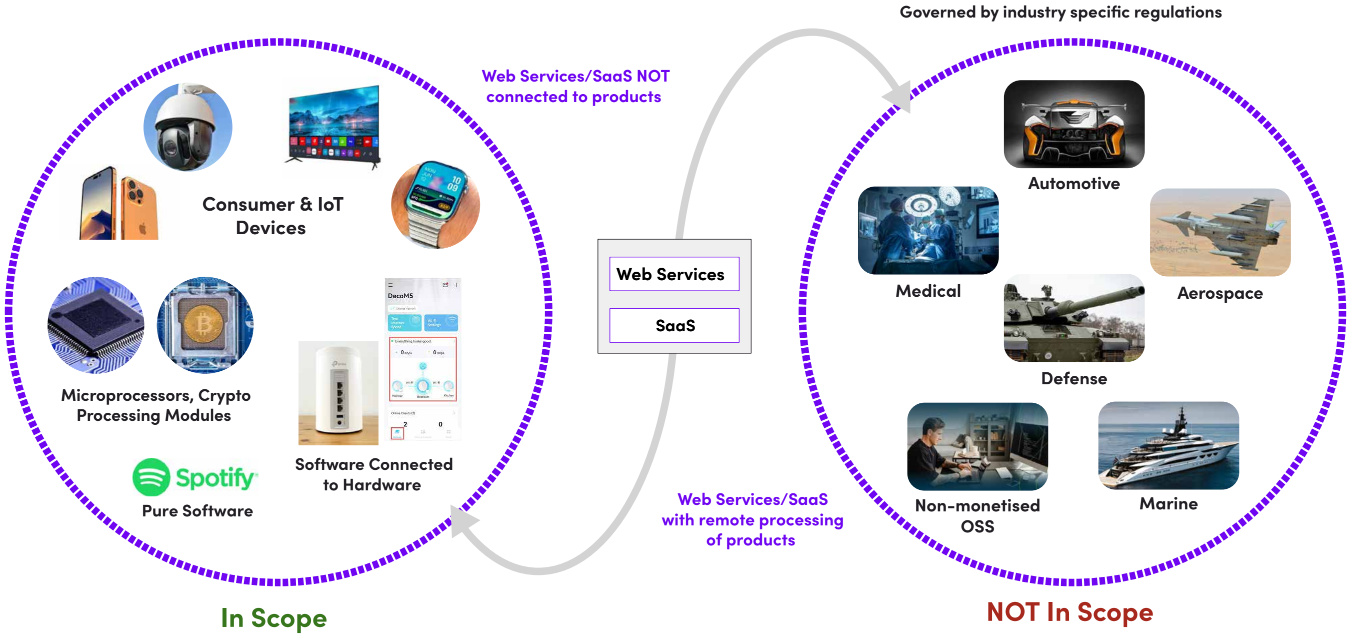
Critical products represent the highest level of cybersecurity risk and include:

- Hardware devices with security boxes
- Smart meter gateways within smart metering systems
- Other devices for advanced security purposes, including for secure cryptoprocessing
- Smartcards of similar devices, including secure elements

These products must have a **European Cybersecurity Certificate** with at least a “substantial” assurance level, reflecting their critical role in security-sensitive environments.

For further information on the technical descriptions for each product category, refer to the Commission Implementing Regulation on the technical description of categories of important and critical products with digital elements pursuant to Regulation (EU) 2024/2847 of the European Parliament and of the Council.

This diagram illustrates, at a high level, the types of products that fall within the scope of the CRA and those that do not.


Governed by industry specific regulations
Web Services/SaaS NOT connected to products
Consumer & IoT Devices
Microprocessors, Crypto Processing Modules
Software Connected to Hardware
Spotify
Pure Software
Web Services
SaaS
Web Services/SaaS with remote processing of products
Automotive
Medical
Aerospace
Defense
Non-monetised OSS
Marine
In Scope
NOT In Scope

What is not covered by the CRA?

The CRA has some exclusions. Products already governed by **industry-specific regulations,** such as medical devices, automotive systems, aviation, and marine equipment, are not in scope, as they are covered by separate regulatory frameworks.

Software-as-a-Service (SaaS) and web services are also not in scope unless they form part of the remote data processing of a physical product placed on the market. Standalone SaaS offerings that are not tied to a product generally fall outside the CRA.

Open source software considerations

Open source software developed in the course of a non-commercial activity is not directly in scope. However, open source software, which is monetised by its manufacturer (eg, through the provision of support services or the like), is in scope.

However, manufacturers who integrate open source software into commercial products remain fully responsible for the security and compliance of the entire product, including third-party open source components: even if the latter are not in scope, manufacturers need to exercise due diligence when integrating them in their products. Consequently, while individual open source developers are not liable if they are not profiting, they may face increased scrutiny regarding documentation, vulnerability handling, and artefacts such as SBOMs.

In this respect, the European Commission may establish voluntary security attestation programmes for open source software, possibly supported or funded by manufacturers.

What about products already on the market?

A common question is whether products released many years ago can continue to be sold in the EU after December 2027 if they are not CRA-compliant. The short answer is **no**.

While a product's initial market placement may predate the CRA, **each new unit sold after December 2027 is considered "making available" under EU law.** Products must therefore comply with current harmonised legislation at the point of sale, not at the time of original release.

In practical terms, this means many existing products will require **substantial software changes** to achieve compliance and remain on the market. Where technical upgrades are not feasible or practical, manufacturers will need to consider controlled phase-out strategies aligned with the 2027 deadline.

Products that are not CRA compliant and are already on the market can continue to receive software updates, as long as those updates are self-contained to bug fixes and security patches. If there is a substantial update, e.g. modifying the device's original intended functions, then the manufacturer is required to bring the device into compliance with the CRA.

Implications of Non-compliance

The consequences of failing to comply with the CRA directly affects a manufacturer's ability to place and continue selling products on the EU market.

If a product does not meet the requirements of the CRA, it **cannot be affixed with the CE mark.** Without a CE mark, the product **cannot legally be sold in the European market.** For manufacturers, this alone represents a significant commercial risk, particularly for products with global supply chains where the EU is a key market.

Authorities can also require recalls of non-compliant products already in circulation. Regulators may issue public warnings, which can damage a company's reputation and lead to long-term loss of customer trust, even after technical problems are fixed.

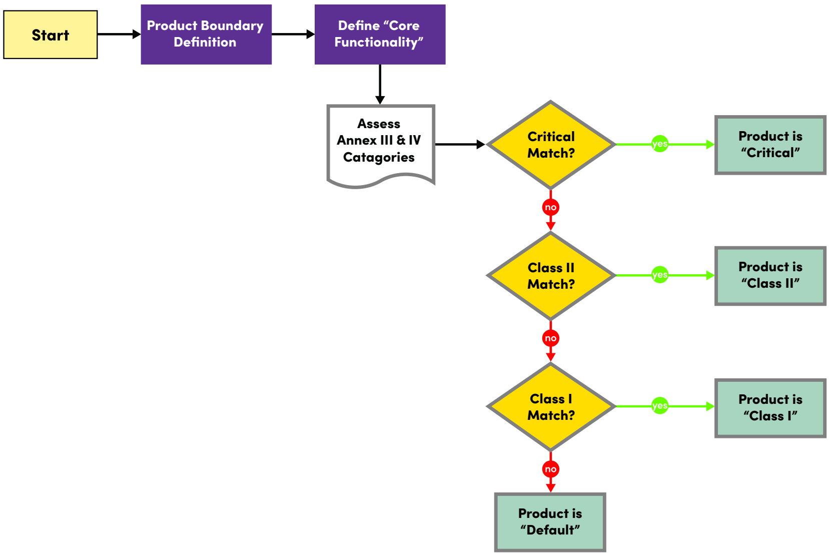
The CRA also brings significant financial penalties. For non-compliance, fines can be **up to €15 million or 2.5% of worldwide annual turnover,** whichever is higher.

There are separate penalties for **giving incorrect or misleading information** to notified bodies or authorities during conformity assessment or compliance activities. In these cases, fines can be **up to €5 million or 1% of worldwide annual turnover.**

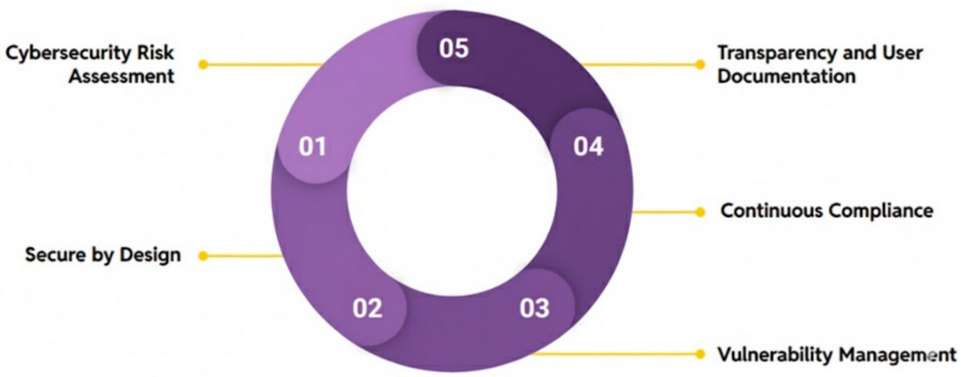
Key Requirements of the CRA

The first step to compliance is identifying the scope of the product and which category of the CRA it falls under. The category determines the conformity assessment route and sets out clear expectations for the requirements manufacturers will need to adhere to.

The following workflow can be used as a general guide to help manufacturers assess their products based on Annex III and Annex IV of the legal text:



The CRA requires manufacturers to meet five key requirements throughout a product's lifecycle. These requirements are closely linked, so you can't fully meet one without addressing the others. The five main requirements are:



Cybersecurity Risk Assessment

Manufacturers must conduct a thorough cybersecurity risk assessment for their products. Under the CRA, this is integral to the design process. A well-executed risk assessment identifies potential attack vectors based on product architecture, intended purpose and reasonably foreseeable use and exposure, allowing appropriate mitigation strategies to be planned early.

A practical approach to cybersecurity risk assessment is to review product requirements, system design, and the user journey, then consider how an attacker might exploit these elements. From there, assess risks to confidentiality, integrity, and availability, as well as the likelihood of exploitation.

The following process outlines the steps to take when conducting a risk assessment:

Identify User Stories

What are the potential attack surfaces from a user perspective when looking at the product requirements and system design

Assess Impact on Confidentiality

Is there confidential data stored on the device? Can this data be compromised based on the attack surface? What is the impact?

Assess Impact on Integrity

Based on the attack surface, can stored data be modified / can the system be tampered with? What is the impact?

Assess Impact on Availability

Based on the attack surface, could the threat destabilise the system, crash services or render the device unusable? What is the Impact?

Determine Exploit Difficulty / Likelihood

Context matters, does the exploit require physical access? How hard is it to gain physical access? What is the likelihood of an exploit happening?

Mitigations & Recommended Actions

What is the best way to mitigate against the potential threat? What provisions can be put in place? Recommended actions should translate into requirements

Consider an example user story involving physical access to a device that stores secure data. In the event a device exposes a physical USB port, a potential attack surface might be:

> **As an attacker with physical access to the device, I can connect a malicious USB device in order to gain unauthorised access to the system**

From this point, we can assess the impact on the Confidentiality, Integrity, and Availability (CIA) principles. Since the device stores sensitive, secure data, unauthorised access can give an attacker visibility into it. Additionally, the attacker may be able to modify the data or render it unusable by an authorised user, all of which combined make the CIA element a **high** risk.

The difficulty or likelihood of exploitation depends on where the device operates. For example, if the device is situated somewhere publicly accessible, the risk of exploitation is high. However, if the device is located in a place that is not easily accessible, such as requiring multiple levels of authentication before physical access is possible, then the chance of compromise drops to medium or low.

After determining impact and likelihood, you can consider ways to reduce risk. For example, remove the port if authorised users don't need it, or add USB authentication controls to detect approved devices. These actions then become part of the product's security requirements.

Secure By Design

Under the CRA, manufacturers must ensure that products are designed with security in mind from the very beginning of the development cycle. Security cannot be treated as a late-stage add-on or a post-launch concern. It must be integral to the product architecture, system design, and development process.

The right level of security is not set by a fixed checklist but by the results of the cybersecurity risk assessment. Threat modelling and risk analysis help identify likely attack vectors and their impact, and these findings are used to set security requirements and design choices. In practice, secure-by-design activities and risk assessment often happen together and are updated as the product develops.

While the specific mitigations will vary depending on product type and risk profile, several common design principles and technical measures are typically expected.

A foundational example is **secure boot.** Ensuring that the device boot chain only executes cryptographically verified and trusted firmware prevents malicious or unauthorised code from running during early boot. This establishes a hardware root of trust that protects the system from boot.

Encryption is another core element. Data must be protected both at rest and in transit to preserve confidentiality and integrity. This applies not only to user data, but also to credentials, configuration data, and any sensitive operational information stored or transmitted by the device.

Products may also enhance security by **minimising attack surfaces** - products may expose physical interfaces, such as USB, Ethernet, or debug ports. Where such interfaces are present, they must be explicitly secured. This can include restricting access through firewall rules, whitelisting permitted devices or protocols, or disabling unused interfaces entirely. In addition, attack surfaces can be minimised by implementing the principle of least privilege, securing applications internally, and removing any applications that are not necessary for the device to function as intended.

Finally, secure-by-design must account for the fact that vulnerabilities will be discovered after a product is released. Therefore, an **update mechanism** is a core design requirement. Devices must be capable of receiving and applying security updates reliably and under controlled conditions, allowing newly discovered vulnerabilities to be addressed throughout the product's supported lifetime.

Taken together, these measures ensure that security is embedded into the product architecture itself. Under the CRA, secure by design is not about implementing every possible control, but about demonstrating that design choices are driven by documented risk and that foreseeable attack vectors have been addressed.

Vulnerability Management and Continuous Compliance

The CRA requires manufacturers to implement processes to identify, address, and manage vulnerabilities **throughout the entire product lifecycle,** not just at the point of release. Effective vulnerability management under the CRA is inherently continuous and depends on maintaining long-term visibility and control over a product's software supply chain.

A **Software Bill of Materials (SBOM)** is key to this effort. An SBOM provides a complete inventory of a product's software components, including versions and provenance, and forms the basis for assessing exposure to known vulnerabilities. Without this visibility, meaningful vulnerability management and ongoing compliance are not possible.

Once an SBOM is in place, components must be **continuously monitored** for known vulnerabilities. This allows manufacturers to understand both the presence and severity of applicable CVEs at any point in time, including after products have been deployed in the field.

Vulnerability management extends beyond detection. Manufacturers must ensure that vulnerabilities are addressed promptly and that **security updates** can be delivered reliably to deployed products. This requires update mechanisms that remain operational and secure throughout the product's supported lifetime.

The CRA also introduces explicit obligations around **incident response** for actively exploited vulnerabilities and severe incidents impacting PDEs. Manufacturers are required to submit an early warning notification to the Computer Security Incident Response Team (CSIRT) via the CRA Single Reporting Platform (SRP) within 24 hours of becoming aware of the incident. The information is also made available in parallel to the European Union Agency for Cybersecurity (ENISA).

Within 72 hours, a full notification must be issued, and a final report must be submitted no later than 14 days after a corrective measure is implemented for actively exploited vulnerabilities, and within a month for severe incidents. Meeting these deadlines requires incident response and reporting processes to be clearly defined, tested, and maintained in advance.

Together, vulnerability management and continuous compliance make sure product security stays strong after release. Manufacturers must be able to demonstrate that monitoring, remediation, update delivery, and incident response processes remain active and effective as long as the product is on the market.

Transparency and User Documentation

The CRA requires manufacturers to provide clear, accessible documentation on their products, including security features, known limitations, and how vulnerabilities are managed. This information must be available to both users and regulatory authorities.

Manufacturers must document the product's intended purpose and provide instructions for use, making sure the product is deployed and operated in line with its security assumptions.

Clear information must also be provided on vulnerability handling, including how vulnerabilities are monitored and how users or external parties can report potential security issues. An SBOM may be part of the documentation set, providing visibility into the software components that make up the product.

Manufacturers are required to clearly communicate the support and maintenance period for each product, so users understand how long security updates and maintenance can be expected.

Documentation must also describe key security features, such as how data is stored and protected, which encryption methods are used, and which network interfaces or ports are exposed. Reports from tests and assessments used to verify CRA compliance must also be available.

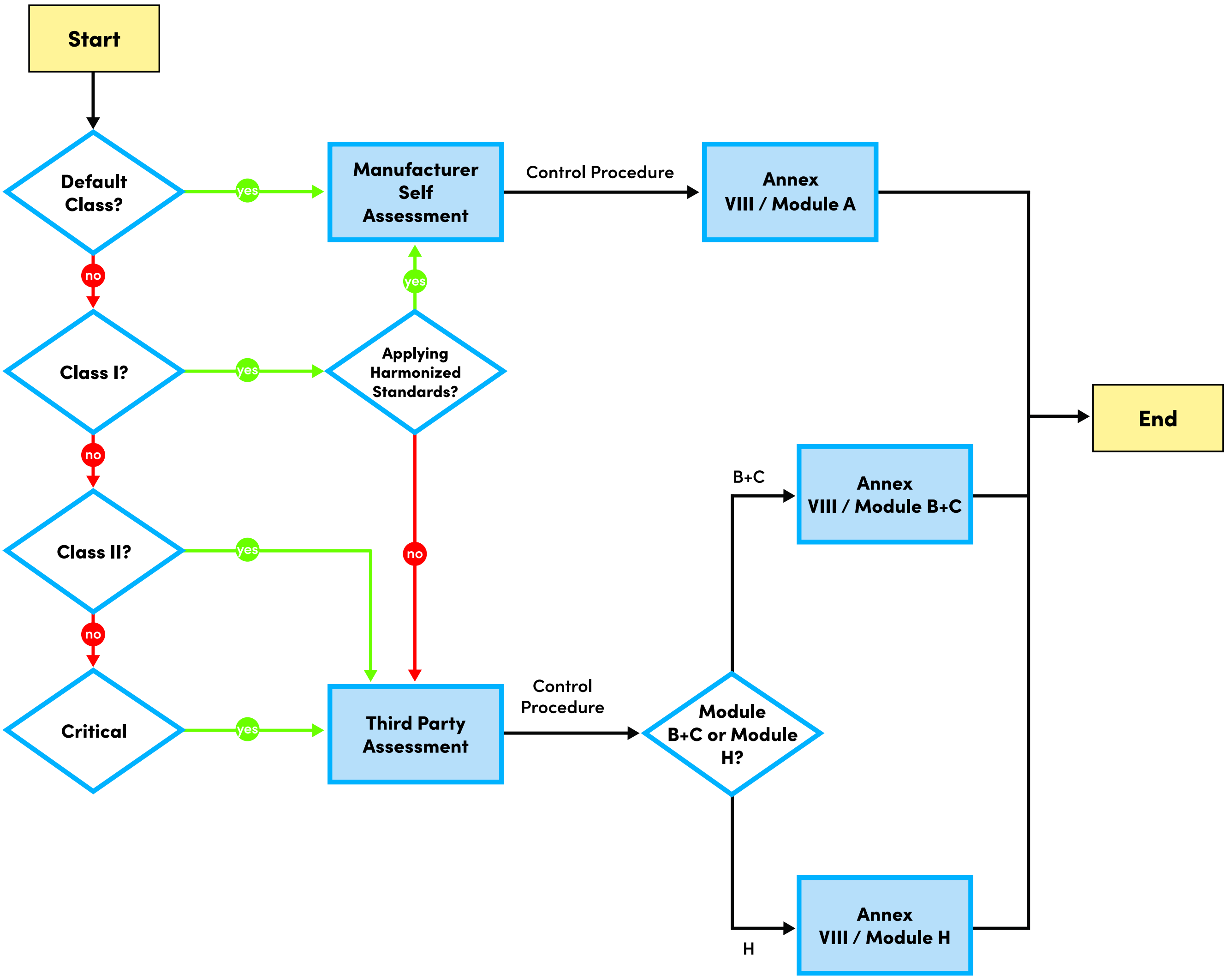
Obtaining CE Marking

Products within the scope of the CRA must affix a **CE marking** before they can be placed on the EU market. The CE marking indicates that a product conforms to applicable EU legislation and, in this context, that it meets the CRA requirements.

Drawing up a CE Declaration of Conformity requires manufacturers to demonstrate that essential CRA requirements have been met, that the appropriate conformity assessment procedure has been followed, and that supporting technical documentation has been produced.

The CRA allows for different conformity assessment routes depending on product classification and standards applied. In some cases, manufacturers may perform **a self-assessment** using the internal control procedure defined in Annex VIII of the CRA official documentation. In other cases, a **third-party conformity assessment** is mandatory and must be carried out by a notified body in accordance with the procedures set out in the CRA.

To help clarify how these assessment routes are selected in practice, the decision flow below summarises the relationship between product classification, the use of harmonised standards, and the applicable conformity assessment procedure under the CRA.



Preparing for the CRA

To prepare for the CRA, a coordinated programme spanning product development, security, legal, and operational teams is required. The earlier manufacturers start, the easier it is to embed compliance into existing workflows rather than retrofitting it under time pressure.

The first step is to **understand the CRA requirements and product classification.** Manufacturers should review the CRA regulations published in the Official Journal of the European Union, understand the relevant timelines, and determine their products' classification. As details continue to evolve, it is also essential to stay informed about regulatory updates and guidance.

Manufacturers should then **conduct a cybersecurity risk assessment** for each product. This includes generating a threat model, identifying potential attack vectors, and assessing their severity. Third-party software must be evaluated using an SBOM, which then serves as the baseline for tracking and addressing vulnerabilities. Ensuring the provenance of all software components is critical to securing the software supply chain.

Based on the outcomes of the risk assessment, manufacturers must **implement appropriate security features.** This includes embedding secure-by-design principles into the product architecture, following secure software development practices, and using automated tools to detect security issues during development. Products must also include a reliable software or firmware update mechanism to address vulnerabilities after deployment. Where appropriate, penetration testing can be used to validate that implemented controls are adequate.

Beyond product design, manufacturers need to **establish processes for vulnerability management.** This includes tooling to track vulnerabilities across the software stack, defined patching processes, and a clear incident response plan that supports the CRA's reporting timelines. Manufacturers must also provide a mechanism for users or external parties to report potential security issues.

Preparing for the CRA also requires **clear ownership**. Compliance typically spans engineering, IT, security, and legal teams, making it essential to define roles and responsibilities early. Manufacturers should identify where external expertise may be required and ensure that adequate budget and resources are allocated to the programme.

Finally, manufacturers must ensure **ongoing transparency and continuous compliance.** Documentation must be accurate, accessible, and kept up to date, while products must be continuously monitored and maintained throughout their supported lifetime. Regular reviews and, where appropriate, third-party audits can help validate that compliance processes remain effective over time.

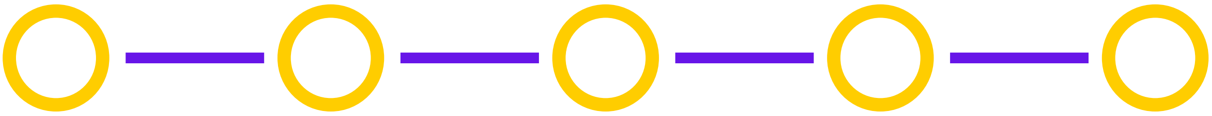
Taken together, these steps allow manufacturers to move from understanding the CRA to actively preparing for it, reducing risk and avoiding last-minute remediation as enforcement deadlines approach.

CRA Readiness with Linaro

The CRA introduces clear requirements across the whole product lifecycle. Many of these requirements align closely with the challenges device makers already face, particularly in security design, vulnerability management, and software supply chain visibility.

Linaro supports manufacturers by applying existing experience and tooling to these areas, helping reduce the effort required to meet CRA obligations in practice. Linaro has world-class expertise in helping manufacturers develop secure, innovative, and compliant products at scale. Linaro has a wealth of experience managing a wide range of hardware platforms, from developing products on the cutting edge to maintaining legacy components to ensure they remain secure and functional. These capabilities are critical to meeting the CRA requirements in the embedded systems domain.

The core offering you can expect from Linaro:



Legal & Technical Consultation

Support with understanding the regulation, defining scope, product categorisation, running a GAP analysis and developing a compliance program.

Cybersecurity Risk Assessment

Expertise in putting together a cybersecurity risk assessment, defining risk mitigations and security requirements.

Securing Your product

Securing your product through our deep knowledge in the secure software development lifecycle.

Keeping your product secure through continuous updates to open source components.

Penetration Testing

Product security validation through our penetration testing services.

Software Supply Chain Management

Software supply chain management services enabling continuous vulnerability monitoring and SBOM generation.

Legal and technical consultation

The CRA is a lot to comprehend, and manufacturers will no doubt have a lot of unanswered questions after digesting the legal text. At Linaro, we have a highly experienced legal and technical team who have been dealing with compliance matters in embedded products for many years. Through our consultation services, we can help you make sense of the regulation, support in classifying your product(s), perform a GAP analysis to assess where products may fall short of the requirements and help establish a comprehensive compliance program to ensure processes are repeatable across product lines.

Cybersecurity risk assessment

The CRA requires manufacturers to assess cybersecurity risks based on product design, usage, and exposure. Linaro has extensive experience conducting cybersecurity risk assessments and threat modelling for embedded products and can support customers in identifying attack vectors, assessing impact, and translating findings into concrete security requirements.

Securing you product

Secure-by-design principles are central to the CRA. Linaro has a proven track record of working with device makers and silicon vendors to implement security features such as secure boot, access control, encryption, and over-the-air (OTA) update mechanisms. This experience can help customers embed security into product architectures early in development, rather than retrofitting controls later.

Securing a product in the initial product development stages is one aspect to consider. The other aspect is keeping products secure over time. Software components of a product eventually reach the end of their support period from the vendor; for example, an embedded Linux-based product may have a vendor-provided board support package(BSP) based on a specific Yocto distribution version, where the support period falls short of the overall product's support period. This could lead to a product running an end-of-life Linux kernel and an outdated, unmaintained BSP. Linaro is a key player in the open source community and has expert capabilities in upgrading Yocto BSPs, porting Linux kernels and applying security patches to open source components. Keeping the BSP up to date throughout the product lifecycle is integral to the CRA, as it ensures that vulnerabilities are managed and do not cause potential risks to the product.

Penetration testing

Penetration testing is a trusted method of ensuring that your product holds up against the security features implemented as part of the risk assessment and secure by design phases. Linaro offers a range of penetration testing services to ensure the security loop is fully closed. Penetration testing reports provide significant evidence to regulators that cybersecurity risk has been well managed throughout the product development lifecycle.

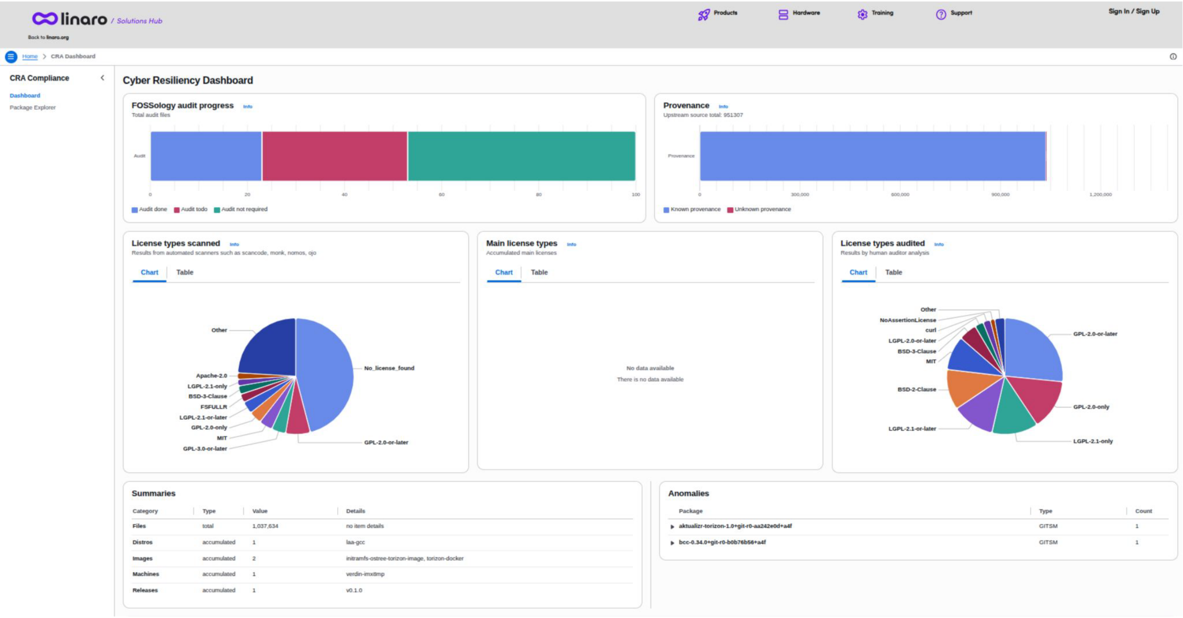
Software supply chain management

Ongoing vulnerability monitoring and post-market compliance are key CRA requirements. Linaro supports this through its software supply chain management capabilities, providing visibility into software components, tracking known vulnerabilities, and supporting continuous monitoring as products evolve.

The CRA also places strong emphasis on documentation and transparency. Linaro can support this requirement by generating SBOMs, dashboards, and reports that provide clear visibility into software composition, licenses, and vulnerability status. These artefacts form a practical foundation for both user-facing documentation and regulatory submissions.

A brief look at Linaro's software supply chain dashboard

The dashboard provides a structured view of the software supply chain, allowing teams to quickly understand what is included in a product, where it came from, and what vulnerabilities may be present.



Cyber Resiliency Dashboard

FOSSology audit progress
Total audit files

Provenance
Upstream source total: 951307

License types scanned
Results from automated scanners such as scancode, monk, nomos, ojo

Main license types
Accumulated main licenses

No data available
There is no data available

License types audited
Results by human auditor analysis

Summaries

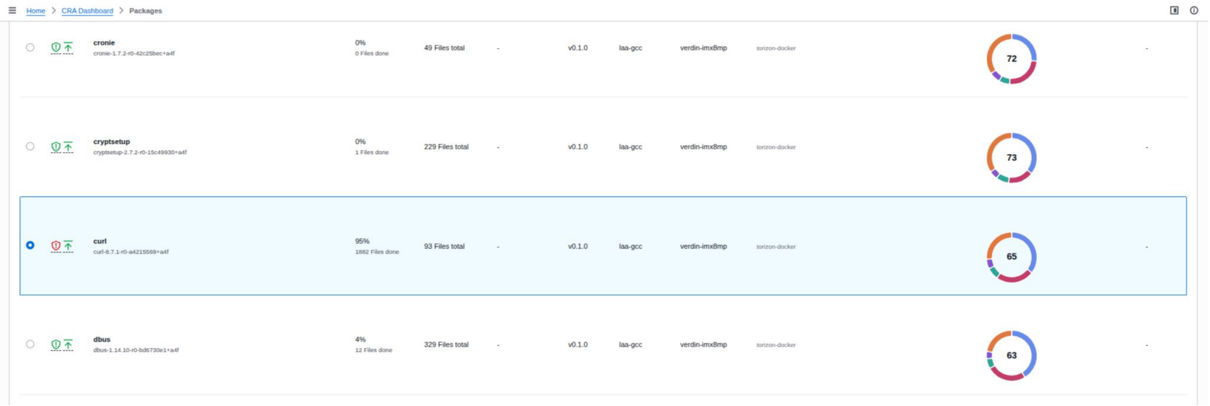
Category	Type	Value	Details
Files	total	1,037,634	no item details
Distros	accumulated	1	laa-gcc
Images	accumulated	2	initramfs-ostree-torizon-image, torizon-docker
Machines	accumulated	1	verdin-imx8mp
Releases	accumulated	1	v0.1.0

Anomalies

Package	Type	Count
▸ aktualizr-torizon-1.0+git-r0-aa242e0d+a4f	GITSM	1
▸ bcc-0.34.0+git-r0-b0b76b56+a4f	GITSM	1

Common use cases include:

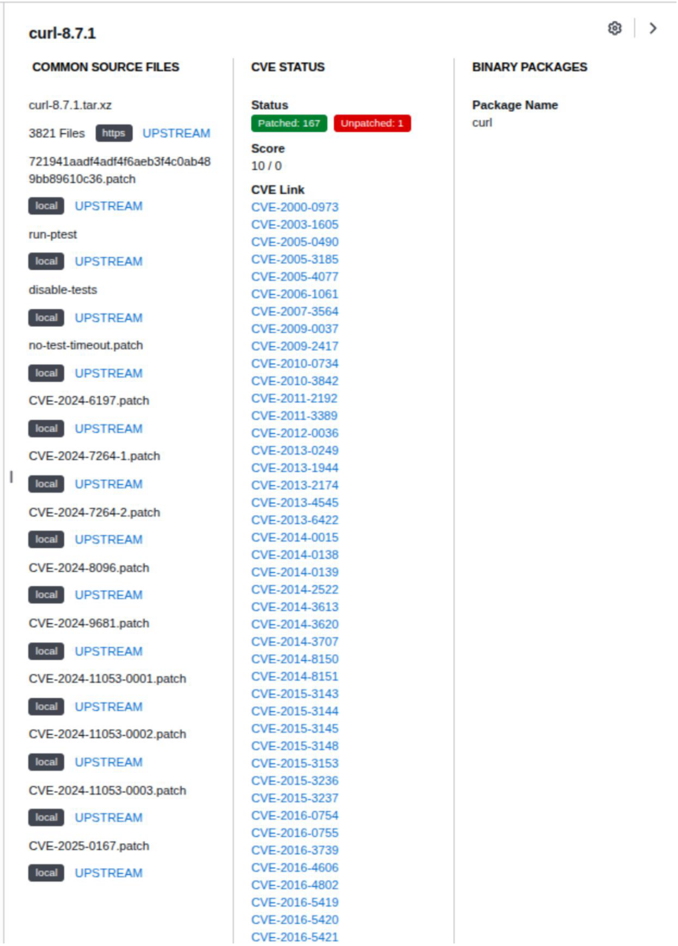
- Reviewing the complete list of software components and versions in a release
- Understanding license distribution and identifying potential compliance risks
- Tracking known vulnerabilities and their status across the software stack
- Linking findings back to upstream sources, patches, and build metadata



≡ Home > CRA Dashboard > Packages

○	cronie cronie-1.7.2-r0-42c25bec+a4f	0% 0 Files done	49 Files total	-	v0.1.0	laa-gcc	verdin-imx8mp	torizon-docker	72	-
○	cryptsetup cryptsetup-2.7.2-r0-15c49930+a4f	0% 1 Files done	229 Files total	-	v0.1.0	laa-gcc	verdin-imx8mp	torizon-docker	73	-
●	curl curl-8.7.1-r0-a4215569+a4f	95% 1882 Files done	93 Files total	-	v0.1.0	laa-gcc	verdin-imx8mp	torizon-docker	65	-
○	dbus dbus-1.14.10-r0-bd6730e1+a4f	4% 12 Files done	329 Files total	-	v0.1.0	laa-gcc	verdin-imx8mp	torizon-docker	63	-

In the example below, we examine the package **curl.** Here we can see the package name, version, link to upstream sources and any patches that have been applied. In addition, we can see all associated vulnerabilities and whether they have been patched. This information helps manufacturers assess per-package vulnerabilities and whether those vulnerabilities are exploitable.



curl-8.7.1

COMMON SOURCE FILES

curl-8.7.1.tar.xz

3821 Files https UPSTREAM

721941aadf4adf4f6aeb3f4c0ab48 9bb89610c36.patch

local UPSTREAM

run-ptest

local UPSTREAM

disable-tests

local UPSTREAM

no-test-timeout.patch

local UPSTREAM

CVE-2024-6197.patch

local UPSTREAM

CVE-2024-7264-1.patch

local UPSTREAM

CVE-2024-7264-2.patch

local UPSTREAM

CVE-2024-8096.patch

local UPSTREAM

CVE-2024-9681.patch

local UPSTREAM

CVE-2024-11053-0001.patch

local UPSTREAM

CVE-2024-11053-0002.patch

local UPSTREAM

CVE-2024-11053-0003.patch

local UPSTREAM

CVE-2025-0167.patch

local UPSTREAM

CVE STATUS

Status
Patched: 167 Unpatched: 1

Score
10 / 0

CVE Link
CVE-2000-0973
CVE-2003-1605
CVE-2005-0490
CVE-2005-3185
CVE-2005-4077
CVE-2006-1061
CVE-2007-3564
CVE-2009-0037
CVE-2009-2417
CVE-2010-0734
CVE-2010-3842
CVE-2011-2192
CVE-2011-3389
CVE-2012-0036
CVE-2013-0249
CVE-2013-1944
CVE-2013-2174
CVE-2013-4545
CVE-2013-6422
CVE-2014-0015
CVE-2014-0138
CVE-2014-0139
CVE-2014-2522
CVE-2014-3613
CVE-2014-3620
CVE-2014-3707
CVE-2014-8150
CVE-2014-8151
CVE-2015-3143
CVE-2015-3144
CVE-2015-3145
CVE-2015-3148
CVE-2015-3153
CVE-2015-3236
CVE-2015-3237
CVE-2016-0754
CVE-2016-0755
CVE-2016-3739
CVE-2016-4606
CVE-2016-4802
CVE-2016-5419
CVE-2016-5420
CVE-2016-5421

BINARY PACKAGES

Package Name
curl

Closing Thoughts

The Cyber Resilience Act represents a shift in how security is expected to be designed, maintained, and demonstrated for connected products sold in the EU. While the requirements are now clearly defined, the real challenge for many manufacturers lies in applying them consistently across real products, teams, and release cycles.

For organisations that already take security and software supply chain management seriously, the CRA is less about adopting entirely new practices and more about making existing ones visible, repeatable, and auditable. For others, it provides a clear framework and deadline for putting those foundations in place.

If you are assessing your CRA readiness, planning next steps, or simply want to sanity-check your current approach against the regulation, Linaro is happy to discuss the problem space and share what we have learned from working with device makers across the industry.

For more information speak with Linaro Experts

About Linaro

In 2010, Linaro was formed to unify a fragmented Arm software ecosystem. Our mission was clear: consolidate the code base to drive innovation on Arm. Today, that vision is a global reality. From Linus Torvalds releasing the kernel on Arm64 hardware to every cloud vendor having an Arm offering, the foundational challenges we set out to tackle have been solved.

As the industry matured, so did we. Linaro has evolved into a Services provider, leveraging our unrivaled Arm expertise to help customers build high-performing, compliant, and sustainable products.

While the way we collaborate has changed, our commitment to the open-source community remains the same. We continue to invest upstream and maintain critical projects, ensuring that every solution we build for our clients also strengthens the broader ecosystem.