CRA EVIDENCE WHITEPAPER

The EU Cyber Resilience Act: a practical compliance guide

Whitepaper for manufacturers, importers, and distributors of products with digital elements.

Prepared by CRA Evidence

Version 1.0

Status Living Document

Basis Regulation (EU) 2024/2847

Change history

This is a living document. It is updated as the regulation, official guidance, and harmonised standards evolve. Each version below records what changed.

Version	Date	Description
1.0	17 May 2026	Initial public release. Covers CRA scope and exclusions, product classification, substantial modification, risk assessment with threat modelling guidance, the 13 product security requirements, the 8 vulnerability handling requirements, technical documentation, conformity assessment routes, and the wider EU regulatory picture.

Contents

Executive summary

IN 60 SECONDS

What it covers: connected hardware and software products placed on the EU market, with security treated as a product compliance requirement rather than best practice.

When it bites: Article 14 reporting from 11 September 2026; full technical, documentation, and CE marking obligations from 11 December 2027.

What you must produce: cybersecurity risk assessment, SBOM, technical file, user instructions, EU declaration of conformity, CE marking, and Article 14 incident and vulnerability reports.

Who needs to act

Manufacturers carry the main burden. Importers and distributors have due-care checks before making products available.

What changes

Cybersecurity becomes part of product compliance: secure design, vulnerability handling, documentation, CE marking, and post-market action.

First deadline

Article 14 reporting starts on **11 September 2026** for actively exploited vulnerabilities and severe incidents.

Full application

Full technical compliance applies from **11 December 2027**. Earlier products are covered after substantial modification, but reporting still applies.

Evidence backbone

The technical file needs the risk assessment, SBOM, support-period rationale, test evidence, user instructions, declaration, and evidence of conformity to the essential cybersecurity requirements.

Conformity route

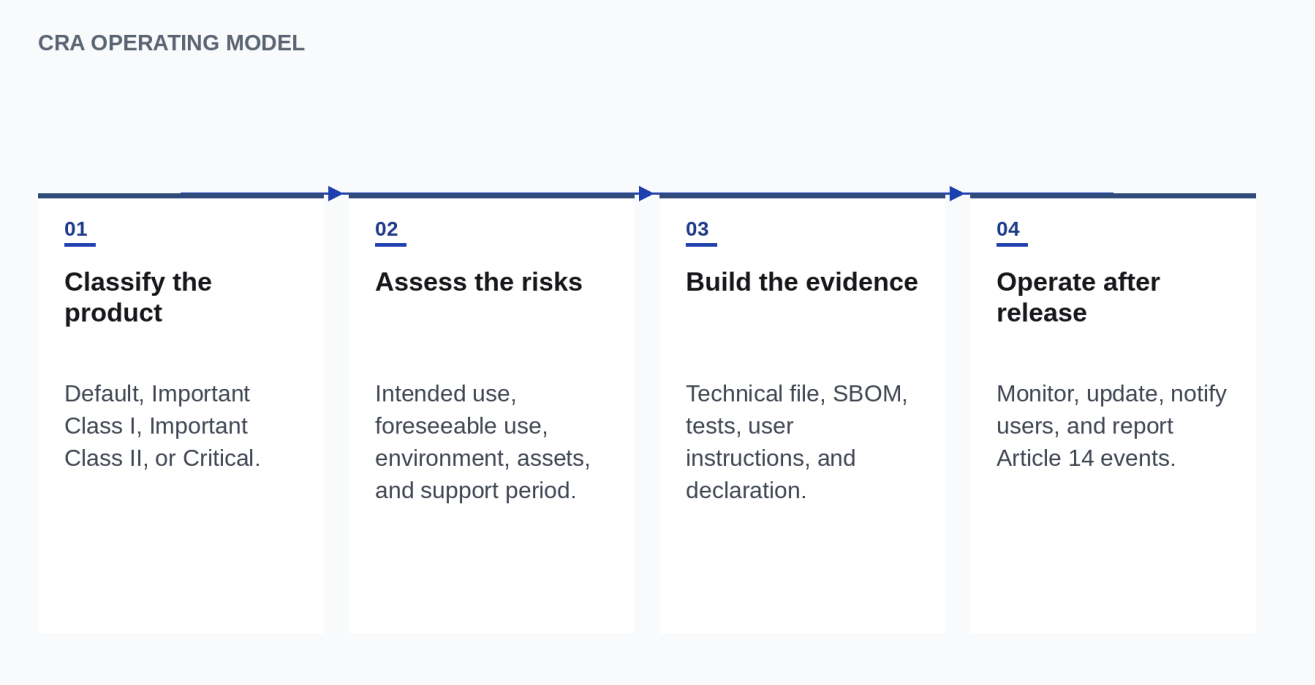
Most products can use Module A self-assessment. Important and Critical products may need a notified body or EU cybersecurity certification route.

What is the Cyber Resilience Act?

Regulation (EU) 2024/2847, the Cyber Resilience Act (CRA), is the first EU-wide framework that makes cybersecurity a binding requirement for products with digital elements placed on the EU market. The authoritative text is available on EUR-Lex.

The CRA applies to manufacturers, importers, and distributors of connected hardware and software. It covers products from consumer IoT devices to industrial control systems. The practical change is simple: cybersecurity now has to be designed, evidenced, maintained, and monitored as part of product compliance.

Non-compliance with the essential cybersecurity requirements or the obligations in Articles 13 and 14 can lead to penalties of up to EUR 15 million or 2.5% of worldwide annual turnover, whichever is higher. Lower tiers apply: up to EUR 10 million or 2% for breaches of other specified obligations, and up to EUR 5 million or 1% for supplying incorrect, incomplete, or misleading information to notified bodies or market surveillance authorities. Market surveillance authorities can also require corrective action, restrict availability, withdraw products, or require recalls.



Key dates for compliance planning

The CRA entered into force on **10 December 2024**. The practical compliance work then phases in through three main milestones: notified-body rules in **June 2026**, reporting in **September 2026**, and full technical compliance in **December 2027**.

NOTE

Current Commission guidance: The European Commission published draft CRA guidance on 3 March 2026. The consultation closed on 13 April 2026. It is not final, but it is useful planning material for market placement, free and open-source software, support periods, substantial modification, product classification, component due diligence, remote data processing, vulnerability handling, and overlaps with other EU legislation. AI Act and DORA boundary questions may still need further guidance.

10 December 2024

Entry into force

Transition period starts

11 June 2026

Notified bodies

Chapter IV applies

11 September 2026

Reporting

Article 14 reporting starts

11 December 2027

Full application

Technical requirements, CE marking, documentation and conformity assessment

DO THIS FIRST

Start with reporting readiness. The Article 14 deadline arrives before full technical compliance, and it applies to products that are already on the EU market.

Because reporting starts on **11 September 2026**, reporting readiness should be the first implementation workstream: **detection, triage, user notification, and authority reporting** need to work before full technical compliance is due.

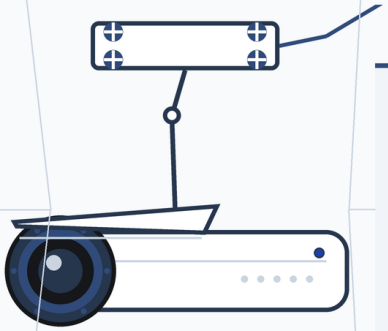
Products placed on the market before **11 December 2027** are subject to the CRA's technical requirements only if they undergo a **substantial modification** from that date. Reporting is different: Article 14 applies to **all in-scope products**, including products already on the EU market.

The CRA across the product lifecycle

STEP 01
Plan product scope
Scope, classification, support period, risk assessment

STEP 02
Develop securely
Secure defaults, secure code analysis, SBOM, dependency control

STEP 03
Validate and document
Security tests, vulnerability triage, technical file, user instructions



STEP 04
Release to market
EU declaration of conformity, CE marking, release decision

STEP 05
Monitor and update
CVEs, advisories, exploit activity, security updates, disclosure

STEP 06
Support and cooperate
Article 14 reporting, user notices, authority requests, end-of-support

A connected IP camera, from product planning to post-market support under the CRA

Which products are in scope

Scope and exclusions

The CRA applies to hardware and software products whose intended or reasonably foreseeable use includes a direct or indirect data connection to a device or network. That includes computers, smartphones, networking equipment, IoT devices, industrial control systems, and data-processing applications.

The following categories are explicitly excluded:

- Medical devices and in vitro diagnostic medical devices covered by Regulations (EU) 2017/745 and 2017/746
- Automotive systems covered by Regulation (EU) 2019/2144
- Aviation equipment covered by Regulation (EU) 2018/1139
- Marine equipment covered by Directive 2014/90/EU
- Products developed solely for national security or defence purposes
- Purely mechanical products with no digital elements or network connectivity

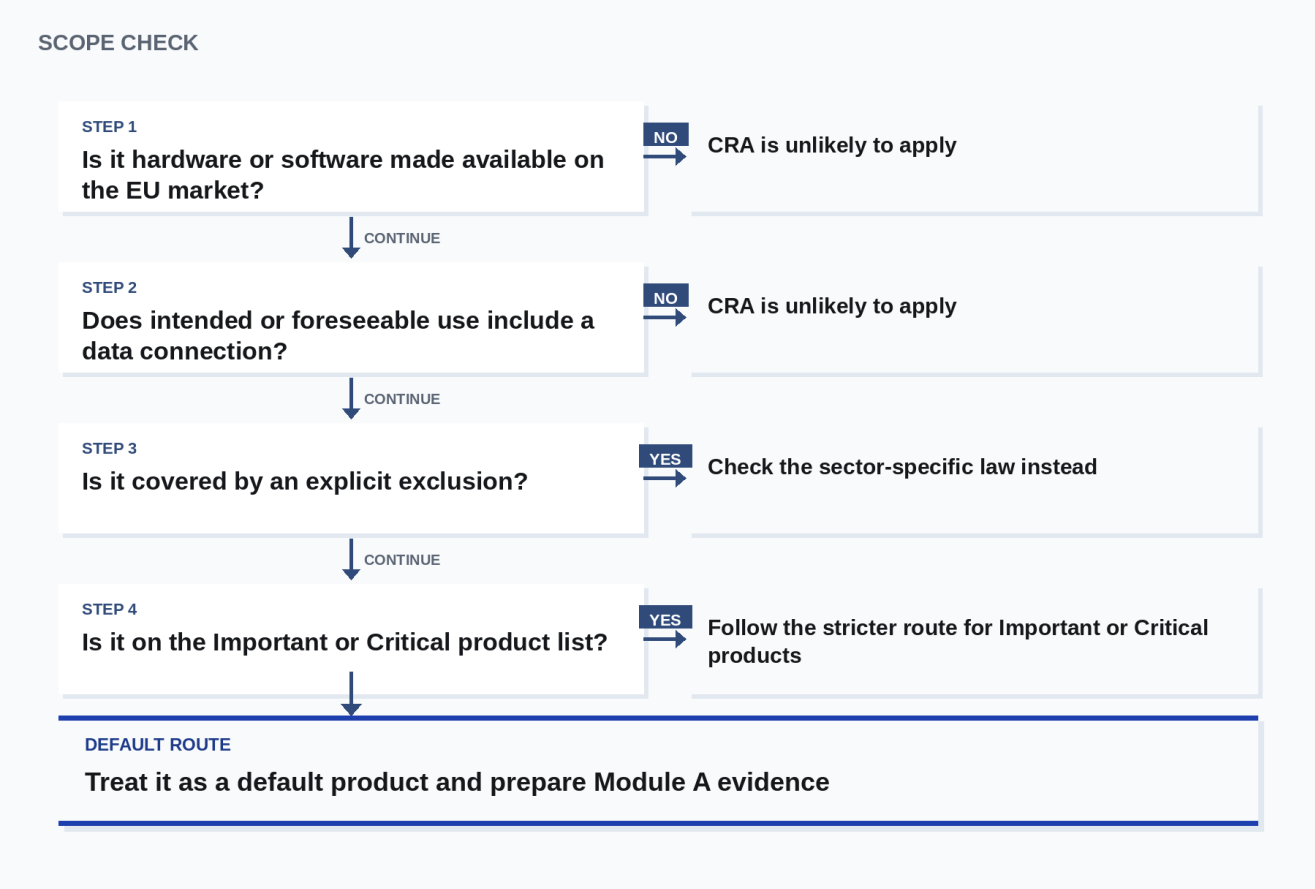
Unless a clear exclusion applies, assume your connected product is in scope.

NOTE

Tailor-made products: a narrow carve-out. If you build a product fitted to one particular business user, under a written agreement between you and that user, you can deviate from two requirements only: the secure-by-default configuration (you must still offer a path back to a secure original state) and the free-of-charge security updates (the agreement can set a different commercial basis). Everything else applies in full: vulnerability handling, the other product security requirements, Article 14 reporting, technical documentation, CE marking, conformity assessment, and the support period. This is not a general B2B carve-out; it does not cover off-the-shelf products sold to businesses.

ECONOMIC OPERATOR RESPONSIBILITIES

Manufacturer	Design secure products, assess risk, prepare technical documentation, run conformity assessment, handle vulnerabilities, report Article 14 events.
Importer	Check manufacturer compliance, verify CE marking and documentation, keep the declaration available, act on known vulnerabilities.
Distributor	Check due-care indicators before supply, verify required information and instructions, avoid making non-compliant products available.



Product classification drives the assessment route

Your product category determines how you demonstrate conformity.

Category	Examples	Conformity assessment
Default "Unclassified"	General software and connected consumer products that are not in the Important or Critical categories	Module A: self-assessment
Important "Class I"	Identity, browser, password manager, antivirus, VPN, network management, router, smart lock, security camera, and similar products	Module A only where applicable harmonised standards, common specifications, or certification schemes are applied as required; otherwise Module B+C or Module H
Important "Class II"	Hypervisors, container runtimes, firewalls, IDS/IPS, and tamper-resistant microprocessors	Module B+C, Module H, or an applicable European cybersecurity certification scheme at least "substantial" assurance level
Critical products	Secure elements, smartcards, smart meter gateways, and hardware security boxes	European cybersecurity certification where required and available; otherwise Class II routes apply

The four product categories

The table above shows examples. The full reference, against which you compare your product's core functionality, is set out below.

Default products

Most products end up here. Any product with digital elements whose core functionality does not match an entry in the Important or Critical lists below is treated as Default. The conformity route is Module A self-assessment.

Common examples:

- Smart TVs and streaming devices.
- Network printers and multifunction office devices.
- Bluetooth speakers and consumer audio products.
- Media player software applications.
- Game consoles, e-readers, and similar consumer electronics.
- Smart kitchen appliances such as ovens, fridges, and dishwashers without security functions.
- Smart light bulbs and connected lighting without security functions.
- Fitness trackers that do not have a health-monitoring purpose.
- General-purpose mobile applications that are not browsers, password managers, or VPN apps.
- Office productivity software such as word processors and spreadsheets.

The list above is illustrative. The Important and Critical lists below are exhaustive.

Important products (Class I)

Mandatory third-party assessment, unless applicable harmonised standards, common specifications, or certification schemes are applied as required.

1. Identity management and privileged access management software and hardware, including authentication and access control readers (including biometric readers).
2. Standalone and embedded browsers.
3. Password managers.
4. Software that searches for, removes, or quarantines malicious software.
5. VPN products.
6. Network management systems.
7. Security information and event management (SIEM) systems.
8. Boot managers.
9. Public key infrastructure and digital certificate issuance software.
10. Physical and virtual network interfaces.
11. Operating systems.
12. Routers, modems intended for connection to the internet, and switches.
13. Microprocessors with security-related functionalities.

14. Microcontrollers with security-related functionalities.
15. ASICs and FPGAs with security-related functionalities.
16. Smart-home general-purpose virtual assistants.
17. Smart-home products with security functionalities (smart door locks, security cameras, baby monitoring systems, alarm systems).
18. Internet-connected toys with interactive features (speaking, filming, location tracking).
19. Personal wearables with health-monitoring purposes (where Regulations (EU) 2017/745 or 2017/746 do not apply), or wearables intended for use by children.

Important products (Class II)

Mandatory third-party assessment, stricter route. Self-assessment is not available even where harmonised standards exist.

1. Hypervisors and container runtime systems that support virtualised execution of operating systems and similar environments.
2. Firewalls, intrusion detection and prevention systems.
3. Tamper-resistant microprocessors.
4. Tamper-resistant microcontrollers.

Critical products

European cybersecurity certification required where the scheme is available. Otherwise the Class II route applies.

1. Hardware devices with security boxes.
2. Smart meter gateways within smart metering systems as defined in Article 2, point 23 of Directive (EU) 2019/944, and other devices for advanced security purposes, including secure cryptoprocessing.
3. Smartcards and similar devices, including secure elements.

If your product's core functionality matches an entry on the Important or Critical lists, you are in that class. If your product integrates one of those entries as a component but its own core functionality is something else, the integration does not change your class.

How to classify: core functionality, not integration

The lists above tell you what the categories are. They do not tell you how to apply them to your product. The CRA's answer is one term: **core functionality**.

Your class is determined by what your product's core functionality is, not by which components it integrates. Match the core functionality against the Important lists and the product is Important (Class I or Class II). Match it against the Critical list and the product is Critical. Match neither and the product is Default. That is the whole test).

The practical safeguard sits in the second sentence of Article 7(1). Integrating an Important component does not push the integrating product into the Important class. Embedding a firewall library in a smart-home hub does not make the hub a firewall. Recital 45 makes the point in plain terms: firewalls and intrusion detection systems are Important class II, but other products that happen to integrate them are not.

Use this sequence to self-classify.

1. **Name your product's core functionality in one sentence.** If you cannot, the rest of the analysis fails. Focus on what the product would not function without.
2. **Check the Important lists above.** A match in Class I or II makes the product Important.
3. **Check the Critical list above.** A match makes the product Critical. A European cybersecurity certification route applies where the scheme is available; otherwise the Class II route applies.
4. **No match on either list.** The product is Default. Module A self-assessment is the route.
5. **Document the reasoning.** A one-page memo with the core functionality statement, the list check, and the chosen route belongs in the technical file.

Two worked examples.

Smart-home hub with an embedded password manager. Core functionality: orchestrating routines across consumer IoT devices in a home. The password manager component, sold separately by its own manufacturer, is an Important class I product in its own right. The hub's core functionality is home automation, not credential management. The hub stays Default.

Operating system by feature set. A product is marketed as a smart-home appliance, but its main functions are hardware and peripheral initialisation, process scheduling, memory management, and a system call interface. That is the core functionality of an operating system. Operating systems are an Important class I product. The product is Important class I, regardless of the marketing.

If your classification lands on a class that surprises the rest of the team, the core-functionality statement needs another pass before you ship.

When the cloud is part of your product

Most products with digital elements lean on something off-device: a cloud backend, a mobile companion app, an over-the-air update server, an authentication portal, a device-management system. The CRA does not treat all of those as your product. It treats them as part of the product only when **both** of two conditions are true:

- The software was **designed and developed by your team, or under your responsibility**.
- The product **would not perform one of its functions** without it.

If either condition fails, the remote service sits outside the product boundary for the CRA. A third-party SaaS that you do not own, even if your product talks to it, is not part of your product. A website that promotes the product but does not support its functions is not part of your product either.

When a remote component is in scope, it is in scope **as part of the product**. The technical file, conformity assessment, declaration of conformity, vulnerability handling, and Article 14 reporting timelines all cover the cloud component along with the device.

Use this matrix to settle the case quickly.

Component	In scope as part of the product?
Mobile companion app that pairs with the device	**Yes.** You designed it, and the device cannot be set up or used without it.
Cloud backend that stores and processes the device's data	**Yes.** You designed it, and the dashboard or main feature does not work without it.
Over-the-air update server	**Yes.** You designed it, and the device cannot receive security updates without it.
Authentication portal that controls access to the device	**Yes.** You designed it, and users cannot log in without it.
Marketing website for the product	**No.** It does not support a product function.
Third-party SaaS the product integrates with (you do not own it)	**No.** Not designed by you. The third-party provider carries its own obligations under NIS 2.
Generic cloud infrastructure your service runs on (IaaS or PaaS)	**No.** Not designed by you. The infrastructure provider falls under NIS 2.

A common pattern: a smart-home device with a mobile app, an update server, and a cloud backend. All three are designed by the manufacturer, and the device cannot perform its advertised functions without them. All three are part of the product. CRA obligations apply to the whole bundle. If the cloud backend then talks to a third-party analytics SaaS, that SaaS is not part of the product. The third-party provider carries its own obligations under NIS 2.

The CRA does not require security measures for the manufacturer's network and information systems as a whole. It requires security for the remote services that are part of the product. The line is the product boundary, not the company boundary.

Your supply chain: who does what under the CRA

The CRA puts the main obligations on you as the manufacturer, but importers and distributors also carry duties that affect how your product reaches the market. Three things matter for you to know.

Who	What they verify before supply	What they do on a vulnerability	When they take over your duties
Importer	CE marking, the EU declaration of conformity, user instructions in the right language, your contact details on or with the product	Tells you without undue delay; tells market surveillance authorities directly if the product presents a significant cybersecurity risk	When they place your product under their own name or trademark, or substantially modify it
Distributor	CE marking, that you and the importer have done your part, that the required documents accompany the product	Tells you without undue delay; tells market surveillance authorities directly if the product presents a significant cybersecurity risk; can stop making the product available	Same trigger as for importers

For a manufacturer this means three practical things:

- Your CE marking, your EU declaration of conformity, and your user instructions must be correct and in the right language at the moment a distributor checks them. Channel partners are required to verify these and can refuse to make the product available if they are missing or wrong.
- You need a clear, low-friction contact path that importers and distributors can use to report vulnerabilities into your vulnerability handling process. They will reach for it.
- Any partner who rebadges, places your product under their own name or trademark, or substantially modifies it becomes the manufacturer for that variant. The full technical-file, conformity-assessment, reporting, and support-period duties move to them for that version. See *When someone else becomes the manufacturer* in the next section for the substantial-modification rule.

Substantial modification: when re-conformity applies

After your product is on the market, the CRA splits later changes into two camps. Most are routine and need nothing extra. Some are substantial. A substantial modification is treated, for CRA purposes, as a new product being placed on the market. That means a fresh conformity assessment, a refreshed technical file, a new declaration of conformity, and CE marking on the new version.

The test is short, and it sits in the definition of substantial modification. A change is substantial if either of these is true:

- It **affects compliance** with the essential cybersecurity requirements.
- It **modifies the intended purpose** for which the product was assessed.

If neither applies, the change is not substantial. Document the reasoning anyway and keep it on file. The analysis is part of the evidence trail.

What does not count as substantial

Two carve-outs do most of the work in practice.

Security updates and bug fixes that decrease cybersecurity risk without changing the intended purpose are not substantial. Patching a known vulnerability, adjusting input validation to close a flaw, or rebuilding a component to address a CVE all sit on this side of the line.

Refurbishment, maintenance, and repairs are not automatically substantial either. They become substantial only if they alter the intended purpose or affect compliance with the essential cybersecurity requirements.

Minor user-interface work stays on the safe side too. Adding a language, swapping an icon set, or polishing a screen layout is not a substantial modification on its own. Adding a new input element that needs adequate input validation can be.

Spare parts

The CRA exempts spare parts in a narrow, specific way. **Identical spare parts**, made to the same specifications as the components they replace, are outside the scope of the Regulation altogether. Functional replacements are not.

Use this matrix to settle the case quickly.

Replacement	Host placed before 11 December 2027	Host placed on or after 11 December 2027
Identical to the original component, same specifications	Spare part outside CRA scope. No obligations triggered by the swap.	Spare part outside CRA scope. No obligations triggered by the swap.
Functionally equivalent, different design or specification	The replacement is a CRA product in its own right. The host has no CRA obligations, because it predates the date of application.	The replacement is a CRA product. Assess whether the swap into the host is a substantial modification of the host using the two-prong test above.

Two practical consequences. First, the exemption depends on identical specification. A wireless module rebuilt on a different chipset is not an identical spare, even if the customer cannot tell the difference. Second, the manufacturer who supplies a functional replacement carries the CRA obligations for that part, regardless of who made the host.

Software updates and feature flags

Software releases are the most common source of substantial-modification questions. The two-prong test still settles them.

A patch that fixes a vulnerability is not substantial. A feature toggle that turns on a capability the product was never assessed for is. A model upgrade that lets the product decide on new categories of input is too. If a release ships both a fix and a new feature, evaluate the feature.

Bundling matters less than substance. Whether a feature update arrives on its own or in the same release as a security patch is irrelevant to the assessment.

If you operate feature flags or staged rollouts, the moment that counts is the enablement for end users in production, not the ship of the binary that contains the flag.

The decision in practice

Use this sequence on every change before it ships.

1. **Does the change modify the product's intended purpose?** If yes: substantial. Re-run the conformity assessment for the new version.
2. **Does the change affect compliance with the essential cybersecurity requirements?** If yes: substantial. Re-run the conformity assessment for the new version.
3. **Otherwise:** not substantial. Document the analysis and continue under the existing technical file.

If the product is in the Important or Critical class and the route required a third-party assessment the first time round, a substantial modification puts you back on the same route. Notify the third party in advance of any change that is likely to be substantial. Self-assessment is not a backdoor for re-classifying an Important product after the fact.

Consequences when a modification is substantial

A substantial modification is treated as a new product being placed on the market. For the manufacturer that means:

- Refresh the technical documentation for the changed version.
- Re-run the conformity assessment along the route the product class requires.
- Issue a new EU declaration of conformity for the modified version.
- Re-apply the CE marking, with the new declaration on file.
- Keep the previous version's documentation for the full retention period. The new version does not erase it.

For software products in particular, you may scope security updates during the support period to the latest version you have placed on the market, provided users of earlier versions can move to the latest version free of charge and without new hardware.

Field units already sold under the previous conformity are unaffected. The obligation attaches to the modified version being made available, not to identical units that pre-date it.

When someone else becomes the manufacturer

If you are not the original manufacturer and you carry out a substantial modification, the CRA treats you as the manufacturer for that version. The full Articles 13 and 14 obligations attach to you. The same rule applies if you place the product on the market under your own name or trademark.

This catches more situations than teams usually expect:

- A systems integrator who ships a customer-specific firmware build with new features.
- A reseller who white-labels a product and changes the marketed intended purpose.
- A service provider who bundles a third-party device with their own firmware.

In each case the actor who made the change inherits the manufacturer obligations for that version: technical file, conformity assessment, reporting, vulnerability handling, and the rest. The "importer" or "distributor" label stops protecting them the moment they cross either line.

What you need to have in place

Use this section as a working checklist. The detailed requirement-by-requirement guidance follows afterwards.

Cybersecurity risk assessment

Before placing a product on the market, you need a cybersecurity risk assessment on file. It is the document that explains, in your own words, why the product is safe to ship and to keep on the market.

The assessment should cover:

- The intended purpose of the product, and the use cases you can reasonably foresee
- The conditions and environment the product will operate in
- The data and functions that need to be protected
- The threats that apply, and the controls you rely on to manage them
- The length of time the product is expected to be in use

How most teams structure it. Credible methodologies converge on the same moves: identify the assets (data the product handles, security material like keys and credentials, functions whose loss would damage users), map where each asset lives or moves, model the threats per asset and environment using confidentiality, integrity, and availability as the dimensions, score impact and likelihood, decide which residual risks to accept and which to mitigate, then re-assess after each round of controls (every new key, certificate, or authentication function is itself a new asset to analyse).

Threat modelling. Step three above is the most technical move and has its own established techniques. STRIDE categorises threats as spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege; widely used, fits most connected products. LINDDUN extends the picture for products that handle personal data, adding linkability, identifiability, non-repudiation, detectability, disclosure of information, unawareness, and non-compliance; useful where the data-protection regime overlaps with CRA duties. PASTA runs a seven-stage process from business objectives through to residual-risk acceptance; useful for complex systems where the attack picture drives the design. None of these is CRA-specific, and the CRA does not require any one of them. Pick the one that matches your product's exposure profile.

Where to find a worked-out methodology. The CRA does not prescribe a method. Germany's Federal Office for Information Security publishes Technical Guideline TR-03183, the most detailed CRA-aligned risk-assessment methodology in public circulation. ENISA publishes broader CRA implementation guidance.

Keep the assessment current throughout the support period. When the threat picture, the components, or the use case change, the assessment should change with them.

Support-period determination

Every product needs a defined support period, and you must publish its end date at the point of purchase. The support period is the window during which you handle vulnerabilities, ship security updates, and keep the technical documentation current.

How long it must be

At least five years. If the product is expected to be in use for less than five years, the support period must match the expected use time. If it is expected to be in use for longer, the support period must reflect that longer use; products such as routers, operating systems, and industrial controllers routinely warrant more than five years.

Factors to weigh

When setting the period, take into account, in a proportionate way:

- Reasonable user expectations for the product
- The nature of the product, including its intended purpose
- Any EU legislation that already sets a product lifetime for this category
- Support periods of comparable products on the market
- The availability of the operating environment the product depends on
- The support periods of integrated components that provide core functions
- Any ADCO or Commission guidance for the product category

The reasoning behind the chosen period must be in the technical file. Market surveillance authorities can ask for it.

What you must publish

State the end of the support period at the time of purchase, with at least the month and the year, in an easily accessible place. Where the product has a user interface, display a notification when it reaches the end of its support period.

Update retention

Each security update made available to users during the support period must remain available for at least 10 years after it is issued, or for the remainder of the support period, whichever is longer.

Component due diligence

A product is made of components. Some you wrote, some you bought, some you pulled from an open-source repository. The CRA treats the product as a whole for compliance, so the components count too. If a vulnerability sits in a component, it sits in your product. If a component does not get security updates, your product does not get them either.

Manufacturers must exercise due diligence on third-party components, including free and open-source ones. The components must not compromise the cybersecurity of the product.

How much due diligence is enough depends on the cybersecurity risk the component carries. A library that handles authentication is not the same as a font-rendering library. Use one or more of these checks, proportional to the risk:

1. **Check for CE marking on the component.** If the component is itself a CRA product and the supplier has shown conformity, the CE marking is on the component. That demonstrates the supplier's own CRA work.
2. **Check the security-update history.** A component that ships regular security updates is a better risk than one that has been silent for years. Look for a release cadence and a recent security-advisory record.
3. **Check the component against vulnerability databases.** The European vulnerability database and public CVE databases tell you what is known about the component. A known CVE without a patch is a red flag.
4. **Run additional security tests.** Where the above is not enough, test the component in your integration context: static analysis, dynamic analysis, fuzzing, or a focused security review.

For components integrated before their own supplier is fully under the CRA (so no CE marking is available yet), use the other three checks instead. The due-diligence obligation does not pause just because the supply chain is still catching up.

Evidence to keep on file

The technical file needs to show your due diligence, not just claim it. Keep:

- A list of third-party components in the product, traceable to versions, including open-source ones. The SBOM is the natural place.
- The supplier security documentation you reviewed: security policies, vulnerability-disclosure programmes, support-period commitments.
- Integration test reports that show the component behaves safely in your product.
- Security clauses in contracts or SLAs with commercial suppliers: vulnerability-notification timelines, support-period commitments, escalation rules.
- A record of the product-level mitigations you added where component due diligence revealed limits: sandboxing, restricted permissions, input validation, network segmentation.

When you find a vulnerability in a component

If your due diligence or post-market monitoring identifies a vulnerability in a component, you must do two things. First, notify the person or entity that maintains the component. If the component is open source, that is the upstream project. Second, address and remediate the vulnerability in your product within the same timelines as any other vulnerability you discover. If you developed a fix, share the code or documentation with the maintainer, in a machine-readable format where applicable.

The CRA does not let you wait for the component maintainer to act before you protect your own users. Your product's vulnerability-handling timeline runs independently of the upstream's.

The 13 product security requirements

Every product with digital elements must meet thirteen baseline security requirements when it goes on the market, and continue to meet them throughout the support period. They are the floor for what cybersecurity means in product terms under the CRA.

The thirteen requirements are:

- No known exploitable vulnerabilities at the time the product is placed on the market
- Secure by default configuration out of the box
- Security updates, including automatic updates with an opt-out
- Protection against unauthorised access
- Confidentiality of stored, transmitted, and processed data
- Integrity of data, firmware, and configuration
- Data minimisation
- Availability and resilience, including against denial-of-service attacks
- No negative impact on other connected devices or networks
- Limited attack surface, including external interfaces
- Reduced incident impact through exploitation mitigation
- Logging of security-relevant activity, with the option for the user to opt out
- Secure and permanent data deletion and portability

Each requirement is unpacked in detail later in the guide, with what it means in practice and the evidence you should keep on file.

The 8 vulnerability handling requirements

Manufacturers also need vulnerability handling processes that run throughout the product's support period:

1. Identify and document vulnerabilities (includes software bill of materials, SBOM)
2. Risk management and timely security updates
3. Regular security testing
4. Notification for security updates and vulnerability disclosure
5. Coordinated vulnerability disclosure (CVD) policy
6. Vulnerability sharing and reporting contact
7. Secure update distribution mechanisms
8. Free security updates with advisory messages

Article 14 reporting timelines

These obligations apply from **11 September 2026**. They apply to manufacturers of in-scope products with digital elements, including products placed on the market before **11 December 2027**. Micro and small enterprises are not generally exempt from reporting. The small-business fine relief is narrow: it only concerns the first **24-hour early-warning deadline**.

The CRA distinguishes three levels of vulnerability status:

- **Vulnerability:** any weakness that could be exploited
- **Exploitable vulnerability:** a weakness that can be used under real-world conditions
- **Actively exploited vulnerability:** one that has been confirmed as used in an attack

When the clock starts

You are not on the clock the moment a signal arrives. The clock starts once you have done an initial assessment and have a reasonable degree of certainty that a vulnerability in your product is being actively exploited, or that a severe incident has compromised your product's security. The emphasis is on prompt initial assessment, not on waiting for the full investigation to close. If a customer, researcher, authority, or other third party brings a potential issue to your attention, assess it without delay and start the clock as soon as that assessment gives you the reasonable certainty.

When you detect an **actively exploited vulnerability**, the following reporting timeline applies:

Timeline	What is required	Where to report
Within 24 hours	Early-warning notification of active exploitation	ENISA via national CSIRT
Within 72 hours	Vulnerability notification: affected product, general nature of the exploit and vulnerability, mitigations, corrective measures users can take, and sensitivity marking where applicable	ENISA via national CSIRT
No later than 14 days after a corrective or mitigating measure is available	Final report: vulnerability description, severity, impact, available information on malicious actors, and details of the security update or other corrective measures	ENISA via national CSIRT

When you detect a **severe incident** affecting product security, the following reporting timeline applies:

Timeline	What is required	Where to report
Within 24 hours	Early-warning notification, including whether the incident is suspected to be caused by unlawful or malicious acts	ENISA via national CSIRT
Within 72 hours	Incident notification: nature of the incident, initial assessment, mitigations, corrective measures users can take, and sensitivity marking where applicable	ENISA via national CSIRT
Within one month after the 72-hour incident notification	Final report: detailed incident description, severity, impact, likely threat or root cause, and applied or ongoing mitigation measures	ENISA via national CSIRT

Notifications are updated as you learn more

The 24-hour, 72-hour, and 14-day (or one-month) submissions are stages of the same notification, not separate filings. Each stage adds the information that was not yet available at the previous one. The CSIRT designated as coordinator can also ask for an intermediate update at any point. You do not need to repeat information you have already provided.

Reports are filed through the **CRA Single Reporting Platform**, routed through the national Computer Security Incident Response Team (CSIRT) in the manufacturer's main Member State, with simultaneous access for ENISA.

Informing your users

After becoming aware, you must inform the impacted users of the vulnerability or incident, and where appropriate all users, of any risk mitigation and corrective measures they can deploy. This is not the same as public disclosure. The duty is to get the information to the users who need it to protect themselves, in proportion to the risk. For products used in sensitive or essential environments, limit detailed technical information to the customers concerned while the vulnerability is unmitigated; premature public detail can make exploitation easier.

Once the vulnerability has been remedied or mitigated, broader disclosure may become appropriate to help users verify their products are no longer affected and to raise general awareness. Keep the level of detail and the timing proportionate to the residual risk. If you do not inform users in a timely manner, the CSIRT may step in and provide the information itself where it judges that proportionate and necessary.

Article 14 reporting timelines

Actively exploited vulnerability

24 hours	early-warning notification
72 hours	vulnerability notification
14 days after corrective measure	final report

Severe incident

24 hours	early-warning notification
72 hours	incident notification
one month after 72-hour notification	final report

Corrective action when a product is not in conformity

If you know, or have reason to believe, that a product you have placed on the market, or one of your processes, is not in conformity with the CRA's essential cybersecurity requirements, you must act immediately. The duty runs from market placement and for the whole support period.

The three options

1. **Bring into conformity.** Fix the product or the process. For software products this is usually a security update or a process change. Apply the fix to the supported versions.
2. **Withdraw.** Stop making the product available on the market. Pull it from your supply chain and from any retailers, integrators, and resellers that hold stock.
3. **Recall.** Get the product back from users who already have it. Use this where the cybersecurity risk to users is significant and a fix or withdrawal alone is not enough.

The choice is proportionate to the risk, not a fixed sequence. A patchable vulnerability with a working fix usually means *bring into conformity*. A product that cannot be safely fixed in the field usually means *withdraw* and, where it is in active use with a significant risk, *recall*.

What you must also do

- **Notify under the Article 14 chain** when the non-conformity is an actively exploited vulnerability or a severe incident. The reporting timeline is set out above.
- **Inform users** of the non-conformity and of any corrective measures they can apply themselves. See *Informing your users* above for the proportionality rules.
- **Cooperate** with any reasoned request from a market surveillance authority, including providing the technical documentation in a language they can read.
- **Preserve evidence.** Keep the records that show what you found, when you found it, what you did about it, and how you communicated with users and authorities. The technical documentation and EU declaration of conformity must remain available for at least 10 years after market placement, or for the full support period, whichever is longer.

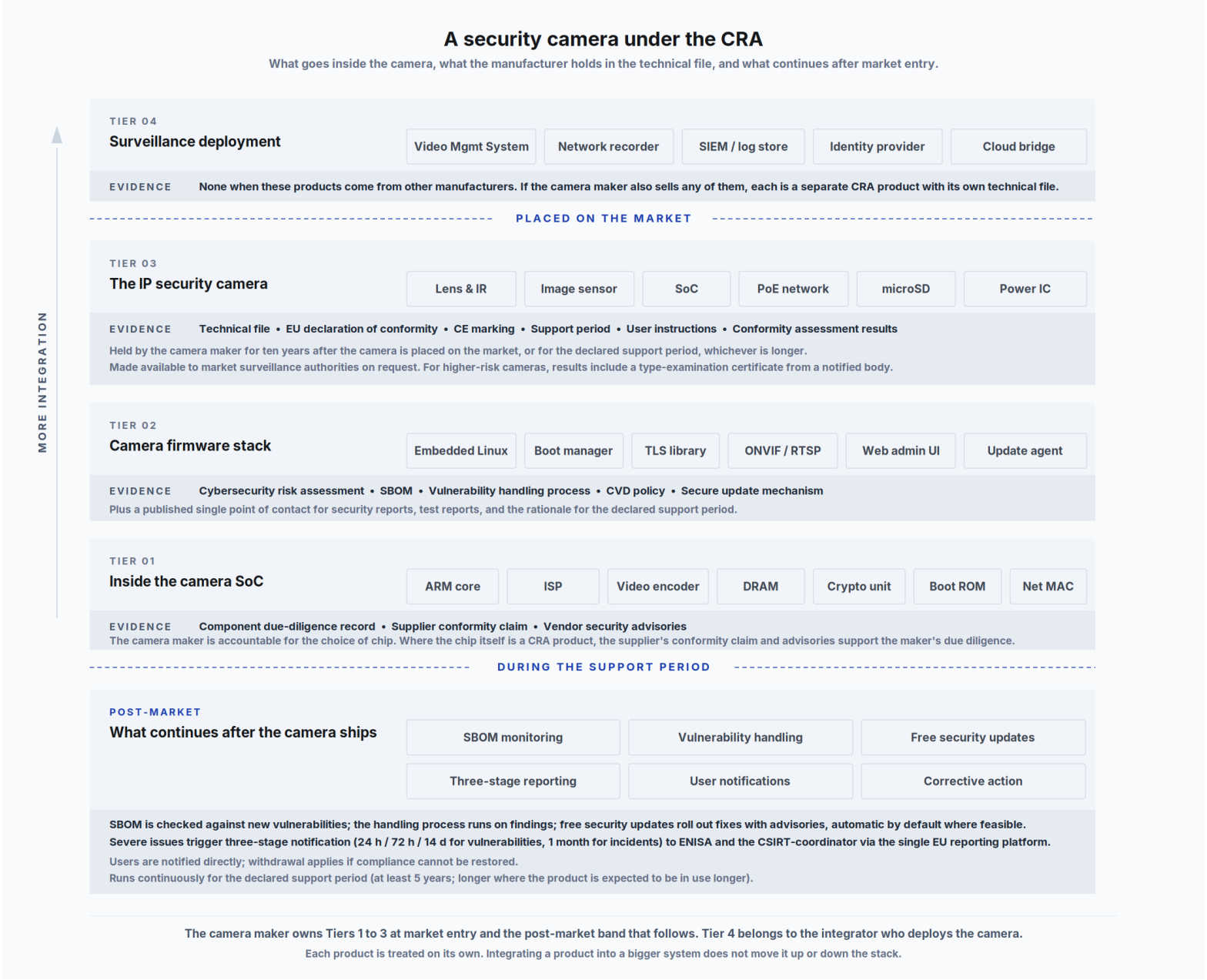
Product documentation requirements

Documentation must be retained for **at least 10 years** after the product has been placed on the market, or for the **full support period**, whichever is longer. At summary level, the technical documentation needs eight evidence families:

1. General product description
2. Design, development and production details (including SBOM)
3. Cybersecurity risk assessment
4. Support period determination
5. Applied harmonised standards and specifications
6. Test reports
7. EU declaration of conformity
8. Full SBOM (on request from market surveillance authorities)

Conformity assessment route checklist

Use the classification table above to identify the route. Then keep the route decision in the technical file together with the standards, specifications, certification scheme, or notified-body evidence used to justify it.



A worked example. The same tier structure applies to every product with digital elements, not just security cameras.

The product security requirements

a. No known exploitable vulnerabilities at time of market placement

Do not ship with publicly known exploitable vulnerabilities that remain untreated. A known vulnerability may come from a public database, a supplier notice, a customer report, or your own internal tracker.

To meet this requirement:

- Check vulnerability databases (including Common Vulnerabilities and Exposures, CVE) before every release
- Use static and dynamic application security testing (SAST/DAST) in your build pipeline
- Perform dependency scanning for all third-party and open-source components
- Document your risk acceptance or mitigation decision for every identified issue

b. Secure by default configuration

The product should be safe to use in its default state. Disable unnecessary services, avoid weak default credentials, and keep any insecure commissioning mode short-lived and controlled. The default-configuration obligation can be varied for tailor-made products supplied to business users by written agreement, but a path back to the original secure state must remain available.

To meet this requirement:

- Disable remote access ports and debug interfaces in default builds
- Enforce strong default authentication mechanisms
- Restrict administrative functions to authorised users only
- Implement a secure factory reset that restores all settings and firmware to a known secure state while removing user data

c. Security updates, including automatic updates with an opt-out

The product needs a patching mechanism that can deal with security issues after deployment. Where automatic updates are appropriate, enable them by default and give users a clear way to postpone or opt out.

To meet this requirement:

- Implement cryptographic signing and integrity verification for update packages
- Provide rollback prevention and logging of update events
- Build notification systems that alert users to pending updates
- Allow users to postpone or disable automatic updates through a clear configuration interface

d. Protection against unauthorised access

Access controls need to protect both local and remote interfaces. The goal is to stop unauthorised users from reaching functions, data, configuration, or management surfaces.

To meet this requirement:

- Enforce password complexity policies and strong default credentials
- Implement multi-factor authentication (MFA) where appropriate
- Apply role-based access control (RBAC) and session timeout handling
- Log unsuccessful access attempts, use anomaly detection to flag unauthorised activity, and surface those events for review and reporting

e. Confidentiality of stored, transmitted, and processed data

Sensitive data needs protection at rest, in transit, and during processing.

To meet this requirement:

- Use standardised encryption algorithms (for example, AES-256 for data at rest, TLS for data in transit)
- Apply secure key management practices
- Segregate confidential data from non-critical system components
- Maintain audit logs for all data access events

f. Integrity of data, firmware, and configuration

This requirement covers the system itself (firmware, software, configuration files) and the data it handles (measurements, control commands, user inputs).

To meet this requirement:

- Implement secure boot and signed firmware to ensure only trusted code is executed
- Use runtime verification to detect and report tampering attempts
- Apply cryptographic hashing and digital signatures to protect data integrity
- Build infrastructure capable of generating, distributing, and verifying cryptographic keys across system or organisational boundaries

g. Data minimisation

Collect and process only the data needed for the product's intended purpose. This applies to personal data and technical data.

To meet this requirement:

- Conduct privacy impact assessments or data protection by design exercises to identify unnecessary data flows
- Remove or make optional any unused telemetry, diagnostics, or background data collection
- Implement configurable data collection settings so that extended collection can be turned on or off based on context

h. Availability and resilience, including against denial-of-service attacks

During incidents or attacks, key product functions should remain available or fail in a controlled way.

To meet this requirement:

- Implement circuit breakers, retry logic, fallback mechanisms, and watchdog timers
- Apply resource limits to prevent resource exhaustion
- Use rate limiting and input validation to protect against denial-of-service scenarios
- Apply network-level filtering to block overload attempts

i. No negative impact on other connected devices or networks

The product should not disrupt other systems in the same environment. It should behave predictably and avoid excessive use of shared resources.

To meet this requirement:

- Implement traffic shaping and limit broadcast or multicast use
- Ensure compliance with communication protocol specifications
- Use self-monitoring to detect and prevent disruptive behaviour such as network flooding or resource exhaustion

j. Limited attack surface, including external interfaces

Minimise entry points and exposed functionality. This includes physical ports, wireless interfaces, APIs, debug services, and unnecessary software components.

To meet this requirement:

- Disable unused services, ports, and interfaces in production builds
- Harden system defaults and limit user privileges
- Modularise software architectures to isolate components from each other
- Apply secure software design principles and conduct threat modelling to identify and remove unnecessary exposure

k. Reduced incident impact through exploitation mitigation

Assume some attacks will succeed. The product design should limit how far damage can spread.

To meet this requirement:

- Separate system components and run them in isolated environments using sandboxing or containerisation
- Enforce privilege separation so critical functions run with the minimum permissions required
- Design so that a compromise of one component cannot give an attacker control over the full system

l. Logging of security-relevant activity with user opt-out

Record security-relevant activity, such as access attempts and data modifications, so it can be monitored and audited. Users need an opt-out mechanism where the CRA requires one.

To meet this requirement:

- Implement structured logging (for example, JSON logs with timestamps)
- Provide local log storage with log rotation and options for remote log streaming
- Monitor events such as login attempts, configuration changes, and software updates for anomalies
- Provide a clear user-facing mechanism to disable logging where permitted

m. Secure and permanent data deletion and portability

Users need a practical way to remove data and settings permanently. Where data can be transferred to another product or system, the transfer needs to be secure.

To meet this requirement:

- Implement a secure erase function that overwrites storage regions or cryptographically deletes keys
- Use authenticated and encrypted channels for data portability transfers to prevent exposure during transfer

The vulnerability handling requirements

1. Identify and document vulnerabilities

You need to know which software components are in the product and which known vulnerabilities affect them. A software bill of materials (SBOM) gives you that machine-readable inventory.

To meet this requirement:

- Integrate SBOM generation directly into your CI/CD pipeline so every build produces an up-to-date component inventory
- Use established formats such as CycloneDX, SPDX, or SWID for interoperability
- Run automated vulnerability scanning against CVE listings and databases such as CISA KEV and ENISA EUVD
- Maintain the SBOM as part of your technical documentation throughout the support period and provide it to market surveillance authorities on request

2. Risk management and timely security updates

When vulnerabilities are found, fix them quickly and deliver security updates. Where possible, separate security patches from feature updates so critical fixes can be installed promptly.

To meet this requirement:

- Design your update mechanism so security fixes can be rolled out without requiring a full system update
- Structure software and firmware so critical components can be patched independently
- Deliver updates through secure channels with integrity checks
- Maintain records of update activities to support traceability and demonstrate compliance

3. Regular security testing

Security testing is not a one-time exercise. Test products throughout the lifecycle as threats, dependencies, and product behaviour change. Let the risk assessment drive the type and frequency of testing.

To meet this requirement:

- Conduct penetration testing to simulate real-world attacks
- Apply static and dynamic code analysis to identify security weaknesses
- Use fuzz testing to expose input-handling flaws
- Formally schedule and document security code reviews and architecture reviews, especially after significant design or feature changes

4. Vulnerability intake, CVD policy, and advisories

Covers the intake, coordinated disclosure, and advisory duties (items 4, 5, and 6 of the summary above) which run as one workflow in practice.

The CRA names three separate requirements for how you communicate around vulnerabilities: a way for people to report issues, a coordinated disclosure policy, and an advisory when you ship a fix. Here is what each duty asks for.

Intake

Give reporters a clear, low-friction way in. Publish a visible contact method for vulnerability reporting (dedicated email or web form). Support secure communication, for example by publishing a PGP key. The duty covers reports about your own product and about the third-party components it contains.

Triage

Acknowledge every report, log it in a tracking system, assign for review, and resolve within defined timelines. Send confirmation and status updates back to the reporter. Where the issue sits in a third-party component, route it to the upstream maintainer in parallel with your own remediation.

Coordinated vulnerability disclosure policy

Publish a CVD policy that sets expectations for reporters and partners: contact method, expected response times, what you commit to, what you ask of them. Coordinate disclosure to protect users while recognising the reporter's contribution.

Advisories on fix

Once a fix is available, publish an advisory for the resolved issue. Include the CVE identifier, the affected product versions, a standardised severity rating (for example, CVSS), and clear, accessible information on what users should do. Write in language accessible to both technical administrators and non-technical users.

Delayed public disclosure

You may delay public disclosure only where you have a duly justified reason that the cybersecurity risks of immediate disclosure outweigh the benefits, and only until users have had the opportunity to apply the fix. Document the reasoning.

5. Secure update distribution mechanisms

The update mechanism needs to be reliable and resistant to tampering. Where automatic updates are technically feasible, they reduce the time users remain exposed.

To meet this requirement:

- Transmit updates over secure channels and verify them through digital signatures
- Apply updates in a way that prevents incomplete or corrupted installations
- Use differential or modular updates to reduce disruption and deliver fixes to systems more quickly
- Maintain update logs so users or administrators can verify update status

6. Free security updates with advisory messages

Deliver security updates promptly and at no additional cost, except where a separate agreement exists for tailor-made business products. Each update needs a clear advisory message that tells users what changed and what to do.

To meet this requirement:

- Maintain a distribution system that can notify users directly or apply updates automatically, depending on the product context
- Write advisory messages in language understandable to both technical and non-technical users
- Include severity information in advisory messages where relevant
- Tell users what action to take, such as applying the update, changing a configuration, or watching for symptoms of compromise
- Disseminate security updates without delay once they are available, so users are not left exposed while the fix already exists
- Publish advisories through a manufacturer-controlled channel and link to them from the product's support page

The free-of-charge and without-delay duties run for the length of the declared support period. The tailor-made carve-out changes the commercial basis only; advisory messages still apply.

What goes into the technical file

Technical documentation

The technical documentation is the central proof of CRA compliance. It needs to cover the design, technical, and procedural measures used to meet the essential cybersecurity requirements. It must exist **before market placement** and stay current throughout the **support period**.

Technical file evidence through the engineering workflow

Step 1	**Scope and classify**	Product purpose, intended use, market-placement decision, product class, standards route.
Step 2	**Architecture and risk**	Architecture, data connections, conditions of use, risk assessment, mitigations.
Step 3	**Components and SBOM**	Machine-readable SBOM, third-party components, supplier inputs, vulnerability tracking.
Step 4	**Build, test, update**	Secure defaults, hardening, test reports, secure update mechanism, advisory messages.
Step 5	**Release and support**	User instructions, EU declaration, CE evidence, support-period rationale, update records.

The technical file has eight required components. Together they explain **what the product is**, **how it was built and tested**, **which risks were considered**, **which standards were applied**, and **how it will be supported** once it is on the market. You do not need to copy the legal headings, but each topic must be covered.

No.	Component	What it must contain
1	General product description	Intended purpose and functions, relevant software versions, photos or illustrations (for hardware), user information and instructions
2	Design, development and production details	Architecture description (components and interactions), software bill of materials (SBOM), vulnerability-handling processes (CVD policy, contact point, secure update mechanisms), production and monitoring processes including validation
3	Cybersecurity risk assessment	Documented analysis of product risks, explanation of how each essential cybersecurity requirement applies to the product, mitigation of identified risks
4	Support period determination	Documentation of the factors used to set the support period, such as user expectations, comparable products, and legal guidance
5	Applied harmonised standards and specifications	List of harmonised standards, common specifications, or EU certification schemes applied; indication of whether applied fully or partially; alternative solutions where standards are not applied
6	Test reports	Evidence of conformity for both the product and the vulnerability-handling processes
7	EU declaration of conformity	Copy of the declaration linking the technical file to CE marking obligations
8	Full SBOM (on request)	Market surveillance authorities may require the complete SBOM to verify compliance

A single consolidated technical file may cover the CRA and other applicable EU legislation (for example, the Radio Equipment Directive or ESPR), provided all applicable obligations are included.

EU declaration of conformity

The EU declaration of conformity is the manufacturer's formal statement that the product meets the applicable CRA cybersecurity requirements. Each declaration must include:

- Product name, type, and unique identifiers
- Manufacturer's name and address (or authorised representative)
- Statement of sole responsibility by the provider
- Product description ensuring traceability (optionally with image)
- Explicit statement of conformity with relevant Union legislation
- References to harmonised standards, specifications, or certifications used
- Details of any notified body involved (name, number, procedure, certificate number)
- Signature block: place, date, name, function, and signature of the signatory

Once signed, the declaration is legally binding and confirms the manufacturer's full responsibility for cybersecurity compliance.

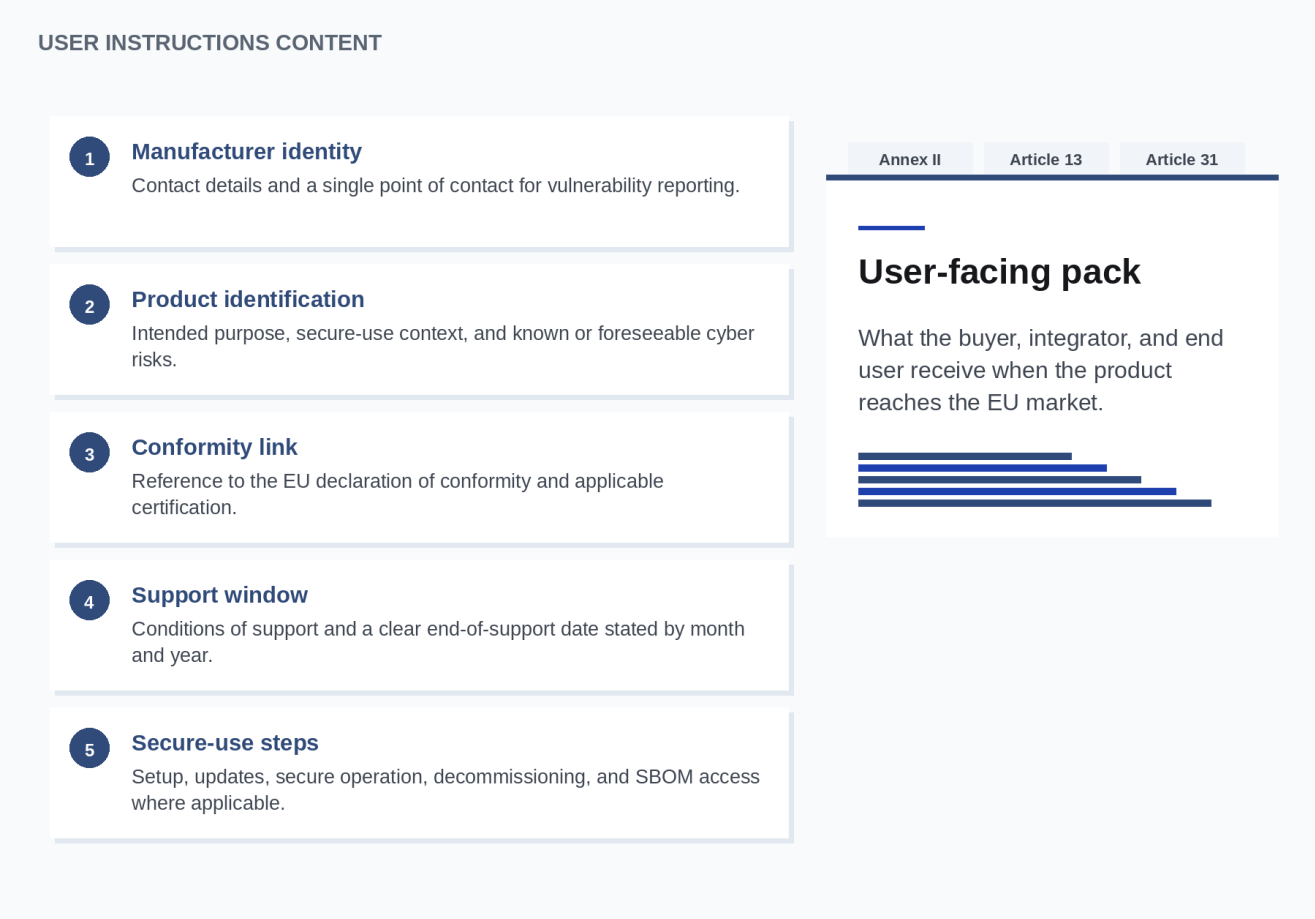
A simplified declaration is permitted for use on packaging or in manuals, in the form: "Hereby, [manufacturer] declares that the product [type/designation] complies with Regulation (EU) 2024/2847. The full text of the EU declaration of conformity is available at: [web address]." This simplified form maintains transparency whilst reducing paperwork, and is particularly useful for small manufacturers or multi-product portfolios.

User information and instructions

User information and instructions are a condition for lawful market placement. Manufacturers must keep instructions available for **at least 10 years** or the **full support period**. Importers and distributors need to check that the instructions exist, are current, and are provided in the right EU language before placing or supplying the product.

The user instructions must contain:

- Manufacturer's identity and contact details
- A single point of contact for vulnerability reporting
- Product identification, intended purpose, and secure-use context
- Known or foreseeable cyber risks
- Link to the EU declaration of conformity
- Support conditions and clear end-of-support date
- Step-by-step security instructions for setup, updates, secure use, decommissioning, and (if applicable) integration and SBOM access



Choosing the right conformity assessment route

Module A: self-assessment

Module A (Internal Control) allows you to self-certify that your product complies with the essential cybersecurity requirements, taking full responsibility for both its design and production. This route is available to manufacturers of default (unclassified) products. It is also available for Important Class I products only where the relevant harmonised standards, common specifications, or European cybersecurity certification schemes are available and applied as required by the CRA route rules.

Under Module A, you must:

- Prepare comprehensive technical documentation
- Detail the product's design, production processes, cybersecurity mechanisms, and vulnerability-handling procedures
- Maintain ongoing responsibility for continued compliance throughout the product's lifecycle
- Implement a plan for security updates and vulnerability management during the product's operational life
- Keep records available for at least 10 years

Modules B and C: product-focused assessment

Modules B and C apply where third-party verification of a specific product type is required. They apply to Important Class I products where the manufacturer has not applied, has applied only in part, or cannot apply relevant harmonised standards, common specifications, or certification schemes. For Important Class II products, the manufacturer must use Module B+C, Module H, or an applicable European cybersecurity certification scheme at least at "substantial" assurance level.

Module B (EU-type examination): A notified body examines a representative product sample and the related technical documentation. It verifies compliance with all essential cybersecurity requirements and issues an EU-type examination certificate when the product design meets the CRA's criteria.

Module C (conformity to type, production control): The manufacturer ensures that all production units conform to the approved type certified under Module B. The manufacturer affixes the CE marking, issues the EU declaration of conformity, and keeps records available for at least 10 years. Together, Modules B and C ensure that a specific product model is technically compliant and that each production batch remains consistent with the approved design.

Module H: process-focused assessment (full quality assurance)

Module H (Full Quality Assurance) focuses on the manufacturer's entire internal quality system rather than individual product testing. It is available for Important Class I and Class II products. Critical products use the certification route where the relevant conditions are met; where those conditions are not met, they use the same routes available for Important Class II products.

Under Module H, you must:

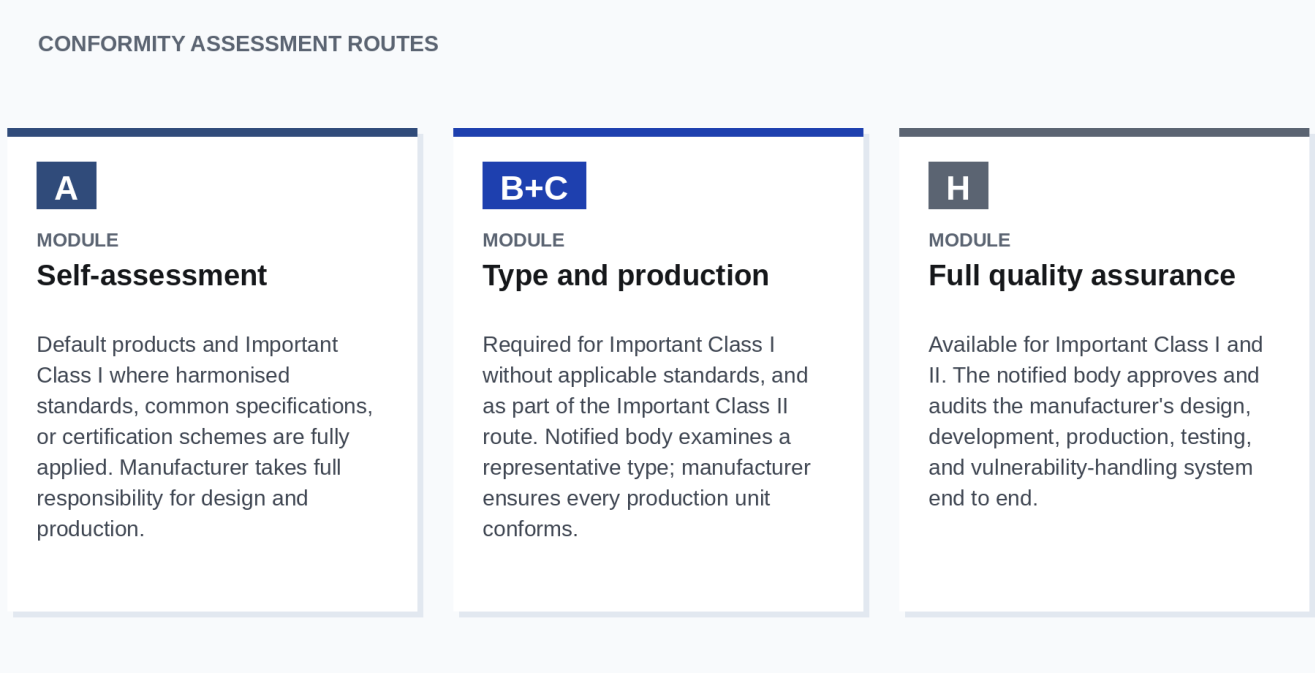
- Establish and maintain a quality system covering design, development, production, testing, and vulnerability handling for the entire product category
- Submit the quality system to a notified body for evaluation and approval

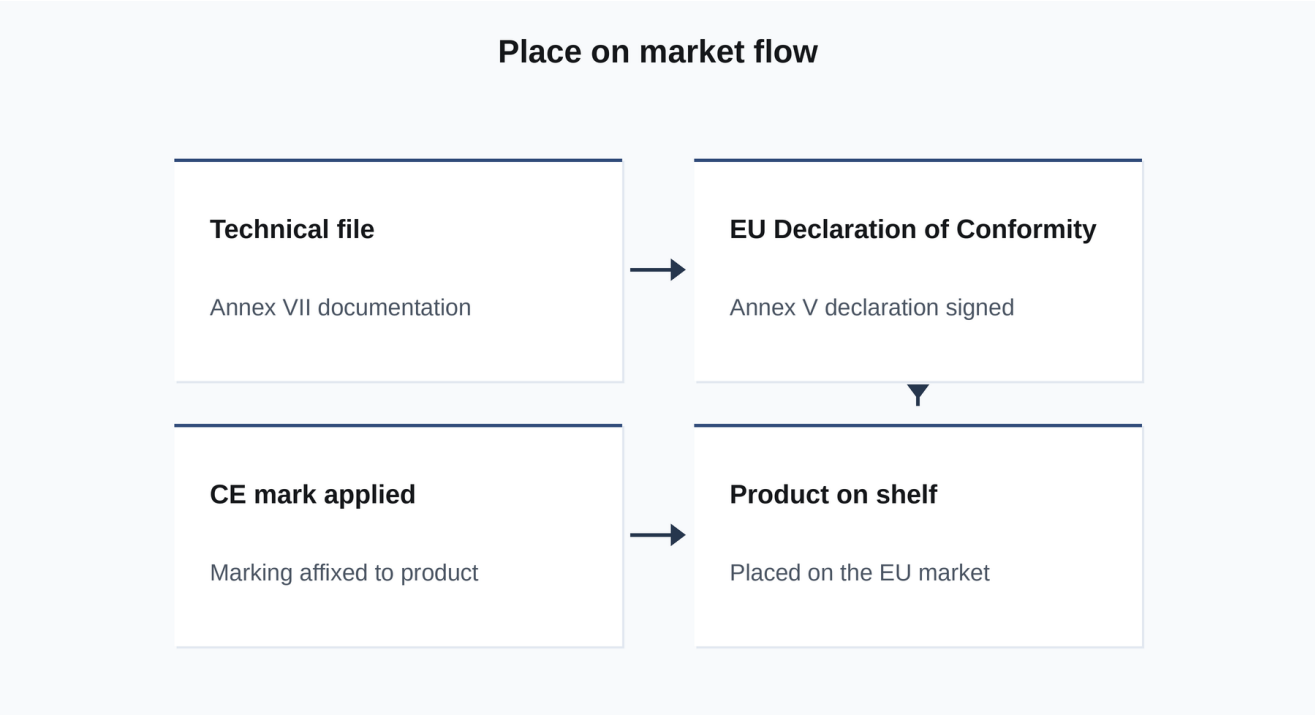
- Accept ongoing surveillance (audits, inspections, and process reviews) by the notified body to verify continuous compliance

Once approved, you may issue declarations of conformity for all products produced under that quality system, without repeating the notified body examination for each individual product type.

The key distinction between routes:

- Modules B+C: focus on the product. A representative product type is tested and certified.
- Module H: focus on the process. The manufacturer's entire design and production system is certified and monitored.





The CRA in the wider EU regulatory picture

The CRA does not sit alone. The question for a manufacturer is practical: where does my CRA work save effort under another EU regime, and where do I still have separate obligations to run in parallel?

Where your CRA work can be reused

- **High-risk AI systems (AI Act, Regulation 2024/1689).** If your product is a high-risk AI system in scope of the CRA, meeting the CRA's essential cybersecurity requirements is deemed to satisfy the AI Act's cybersecurity requirements to the extent covered by your EU declaration of conformity. The conformity-assessment procedure routes through the AI Act regime as a rule, with a carve-out for Important and Critical CRA products. The CRA cybersecurity risk assessment must factor in AI-specific risks such as data poisoning and adversarial attacks.
- **Consolidated risk assessment with other Union law.** The CRA expressly allows the cybersecurity risk assessment to form part of a wider risk assessment required by another Union legal act, where the product falls under both regimes. One assessment artefact, two regulatory uses.
- **One technical file across regimes.** As already noted in the technical-file section, a single consolidated technical file can cover the CRA together with other applicable Union legislation, as long as each regime's obligations are addressed. Useful where the same product already needs documentation under the Radio Equipment Directive, the Ecodesign for Sustainable Products Regulation, or other product law.
- **Shared definitions of refurbishment, maintenance, and repair.** The CRA imports these definitions from the Ecodesign for Sustainable Products Regulation. When you analyse whether a service operation counts as a substantial modification, the Ecodesign definitions are the reference, not a CRA-specific term.

Where separate obligations remain

- **AI Act everything-else.** Cybersecurity is only one slice of the AI Act. Risk classification, transparency, dataset governance, human oversight, post-market monitoring of AI behaviour, and the rest are AI Act duties that the CRA does not address. CRA-conformant cybersecurity is not a presumption of AI Act conformity overall.
- **Ecodesign and digital product passport content.** Ecodesign requirements on energy efficiency, durability, repairability scoring, and the digital product passport's sustainability content are not CRA scope. The CRA evidence trail can sit alongside the Ecodesign work but does not replace it.
- **Data Act IoT data-access rights.** The Data Act gives users contractual rights to access, share, and transfer the data their connected products generate. The CRA covers the security of that data; it does not set the access-rights regime. Different obligation, different evidence.
- **Product liability for defective products.** The Product Liability Directive (2024/2853) keeps strict liability on the manufacturer for damage caused by defective products. The CRA flags that a lack of post-market security updates can be the defect that triggers liability. Your contracts, insurance, and incident playbooks need to account for this exposure independently of CRA conformity.

How CRA Evidence helps

CRA Evidence turns EU Cyber Resilience Act obligations into verifiable product evidence, combining a compliance platform with technical consulting.

Platform

One place to manage the evidence behind CRA readiness:

- **SBOM and component inventory:** CycloneDX, SPDX, and HBOM records for product versions and releases
- **CI/CD evidence automation:** CLI and API workflows for scans, SBOM uploads, release gates, and audit records
- **Signed SBOM and provenance:** versioned evidence, supplier attestations, and due-diligence records
- **Vulnerability operations:** CISA KEV, EPSS, VEX, monitoring, triage, and reporting workflows
- **Technical file and CE evidence:** EU declaration records, retention history, and QR-linked product compliance passports

Technical consulting

Focused support for turning CRA obligations into engineering decisions for your product, architecture, release process, and supplier model.

- **Technical Readiness Sprint:** essential-requirements gap review, architecture recommendations, and a prioritised action plan
- **CRA Programme Lead:** ownership model, obligations tracking, evidence milestones, and technical file maintenance
- **Authority and Incident Response Plan:** reporting workflows, inquiry playbooks, user communications, and evidence-package readiness
- **Regulatory alignment:** connect CRA evidence with Data Act, ESPR, AI Act, RED, and sector requirements
- **Technical workshops:** remote or on-site sessions with product, engineering, security, compliance, and supplier teams

Tool-agnostic: CRA Evidence integrates with CycloneDX, SPDX, Grype, Trivy, CI/CD pipelines, and issue trackers.

A practical first step

Pick one product family. Map the owner, scope decision, SBOM, vulnerability workflow, technical file gaps, and release evidence. That gives the team a concrete CRA baseline without turning compliance into a separate project.

Explore what CRA Evidence covers for your product at craevidence.com. Pricing and plan options are available at craevidence.com/pricing.