FOR ANY MAKER, IMPORTER OR SELLER OF DIGITAL PRODUCTS

Every step to get CRA-ready, *on one checklist.*

A plain-English readiness checklist that walks you from “is this even my problem?” to a signed EU Declaration of Conformity — covering every essential requirement of Regulation (EU) 2024/2847.

This checklist is a practical readiness guide for organisations that design, manufacture, import, or distribute hardware and software products with digital elements in the European Union. It translates the obligations of Regulation (EU) 2024/2847 — the EU Cyber Resilience Act — into a structured, actionable sequence you can work through with your engineering, legal, and compliance teams.

How to use it: Read the Introduction (Chapter 00) to confirm the CRA applies to you and understand the two critical deadlines. Then work through each chapter in order, ticking items as you go. The master checklist in Chapter 06 gives you a single consolidated view for sign-off.

CONTENTS

00

Introduction

What the CRA is, who it covers, and the two dates that matter

What is the Cyber Resilience Act?

The EU Cyber Resilience Act — formally Regulation (EU) 2024/2847 — is a directly applicable EU law that sets mandatory cybersecurity requirements for hardware and software products placed on the EU market. It entered into force on 10 December 2024. The CRA fills a gap that product safety law (Machinery, Radio Equipment, General Product Safety) never addressed: the security of connected and software-embedded products throughout their entire lifecycle, from design to end-of-life.

The core logic is straightforward: if you put a product with digital elements on the EU market, you must ensure it is secure by design, free of known exploits at launch, supported with security updates for a meaningful period, and accompanied by documentation that lets authorities verify all of this. Manufacturers also gain a new ongoing duty to report actively exploited vulnerabilities and severe incidents to a central EU platform.

REGULATION REFERENCE

Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements — published in the Official Journal of the EU on 20 November 2024. It amends Regulation (EU) No 168/2013 and Directive (EU) 2019/1020, and repeals and replaces no prior act (it is a new horizontal layer).

The two dates that matter

The CRA does not have a single compliance date. There are two mandatory milestones that every affected organisation must plan for:

CRITICAL DEADLINES

11 September 2026 — Reporting obligations live.
From this date, manufacturers must report actively exploited vulnerabilities and severe incidents affecting their products to ENISA's Single Reporting Platform within the statutory timelines (24-hour early warning, 72-hour detailed notification, one-month final report). National CSIRTs begin receiving and acting on these reports.

11 December 2027 — Full compliance required.
From this date, all products with digital elements placed on the EU market must meet the essential requirements in Annex I, carry a CE marking, be accompanied by the EU Declaration of Conformity, and have full technical documentation ready for market surveillance authorities. Products already on the market before this date are not retroactively covered, but any new placement or substantial modification triggers compliance.

Who must comply?

The CRA applies across the supply chain for products with digital elements. Your obligations depend on your role:

MANUFACTURER

Full obligations

Designs or manufactures a PDE (or has it designed/manufactured) and places it on the market under their name or trademark — even if sold through others. Bears the full burden: essential requirements, vulnerability handling, technical documentation, conformity assessment, EU DoC, CE marking, incident reporting, support period.

IMPORTER / DISTRIBUTOR

Verify & act duties

Importers must verify the manufacturer's CE marking, EU DoC, and technical documentation before placing products on the EU market. Distributors verify CE marking and accompanying information. Both must act immediately if a product is non-compliant — notifying the manufacturer, market surveillance authorities, and (if necessary) withdrawing or recalling the product.

Open-source stewards face a lighter touch: they must have a cybersecurity policy covering vulnerability handling and co-operate with market surveillance authorities, but the full manufacturer obligations only apply when they place products on the market commercially (i.e., in the course of a commercial activity, even if not for profit).

Authorised representatives (EU-based entities acting on behalf of non-EU manufacturers) take on the manufacturer's compliance obligations towards EU authorities.

How to use this checklist

Work through each chapter in order. Each chapter ends with a chapter-level checklist you can tick as you go. Chapter 06 consolidates the most critical items into a single master list for final sign-off. Use the Interactive Navigator page near the end to jump between chapters quickly if you are returning to a specific section.

INTRODUCTION CHECKLIST

- [ ] **Identified your role** Manufacturer, importer, distributor, or open-source steward — your obligations differ.
- [ ] **Noted the two deadlines** 11 Sep 2026 (reporting) and 11 Dec 2027 (full compliance) are in your project plan.
- [ ] **Confirmed EU market exposure** At least one product is or will be placed on the EU market before 11 Dec 2027.
- [ ] **Assembled a CRA working group** Engineering, legal/compliance, product, and supply-chain stakeholders are involved.

01

Confirm scope & class

Is your product a PDE — and which compliance tier applies?

Does the CRA apply to your product?

The first question every organisation must answer is whether their product is a **product with digital elements** (PDE) as defined in the CRA. A PDE is any software or hardware product and its remote data processing solution that is directly or indirectly connected to another device or network. That definition is intentionally broad: it covers embedded software in hardware, standalone software applications, apps, operating systems, firmware, IoT devices, industrial controllers, consumer electronics, and more.

The key phrase is **connectivity**: a product that has no digital component and no network connection is outside scope. A product with a Bluetooth chip, a USB interface, an API, or an over-the-air update mechanism is almost certainly inside scope.

What is excluded?

The CRA carves out several categories that are already regulated by sector-specific cybersecurity frameworks:

- **Pure SaaS and cloud services** — software offered as a service (where nothing is installed on the user's device) falls under NIS2 (Directive (EU) 2022/2555), not the CRA. However, if the cloud backend is integral to a product's functionality and the product is sold, the combination may be in scope.
- **Medical devices and in vitro diagnostics** — covered by MDR (Regulation (EU) 2017/745) and IVDR (Regulation (EU) 2017/746).
- **Motor vehicles** — covered by UN Regulation No. 155 / UNECE WP.29.
- **Civil aviation** — covered by EASA regulation.
- **Marine equipment** — covered by the Marine Equipment Directive.
- **National security and defence products** — explicitly excluded.

> **SAAS EDGE CASE**
>
> A web application accessed entirely through a browser with no installed component is not a PDE. But if you also ship a desktop client, a mobile app, an SDK, a hardware gateway device, or a firmware update that users install — those components **are** PDEs and bring you into CRA scope. Many "SaaS" companies have at least one in-scope component.

The four compliance tiers

Not all PDEs carry the same compliance burden. The CRA organises products into four tiers based on cybersecurity risk. Your tier determines which conformity assessment route you must use.

Default class (90% of all PDEs) — products not listed in Annex III or Annex IV. Manufacturers may self-assess conformity against the essential requirements using the internal control procedure. Examples: smart TVs, general-purpose software, printers, smart appliances, most IoT devices.

Important Class I (Annex III, first list) — products where a compromise would have significant security impact. Includes: identity management software, browsers, password managers, VPN clients, network traffic monitoring tools, operating systems, routers and switches (consumer), home automation hubs, connected toys with communication features, wearables for health monitoring, smart-home security products (cameras, alarms). Requires conformity assessment against a harmonised standard (or, if none, a third-party assessment).

Important Class II (Annex III, second list) — higher-risk products. Includes: firewalls, intrusion detection and prevention systems (IDS/IPS), tamper-resistant microprocessors and microcontrollers, general-purpose microprocessors intended for use in security-critical systems. Requires a notified body assessment.

Critical (Annex IV) — the highest-risk products where a compromise could have systemic EU-wide impact. Includes: hardware security modules (HSMs), smartcards and secure elements, dedicated smart meter gateways, PKI trust anchors, root certificates. Requires a notified body assessment and, where available, an EU cybersecurity certificate under the EU Cybersecurity Act.

Determine your scope and class — step by step

1. ### List every distinct product

   Enumerate each hardware model, software application, firmware release, and SDK you place (or plan to place) on the EU market. Variants that share the same security design can be grouped.

2. ### Apply the connectivity test

   Does the product connect — directly or indirectly — to another device or network? If yes, it is likely a PDE. If the connection is purely physical (e.g. a passive cable), it is not.

3. ### Check the exclusion list

   Does the product fall under MDR, IVDR, motor vehicle type-approval, EASA, or marine equipment rules? If so, CRA does not apply to that product.

4. ### Check Annex III and Annex IV

   Look up each in-scope product against the Annex III and Annex IV lists. Products not listed are Default class.

5. ### Record the result

   For each in-scope PDE, document: product name, version/model, scope rationale, assigned class, and planned conformity assessment route.

TEMPLATE

Product Scope Register

PRODUCT NAME / MODEL .....

HARDWARE / SOFTWARE / FIRMWARE / SDK .....

CONNECTIVITY TYPE (BT, WI-FI, ETHERNET, USB, CELLULAR, API...) .....

EXCLUSION CHECKED — RESULT .....

CRA CLASS (DEFAULT / IMP. CLASS I / IMP. CLASS II / CRITICAL) .....

CONFORMITY ASSESSMENT ROUTE .....

Maintain one row per distinct product or product family. Keep this register with your technical documentation (required for 10 years under Art. 23).

SCOPE & CLASS CHECKLIST

- [ ] **Inventoried all products** Every hardware, software, and firmware offering destined for the EU market is listed.
- [ ] **Applied connectivity test** Non-connected products are confirmed out of scope with written rationale.
- [ ] **Checked sector exclusions** MDR, IVDR, automotive, aviation, and marine exemptions reviewed and documented.
- [ ] **Assigned a CRA class** Each in-scope PDE is mapped to Default, Important Class I/II, or Critical.
- [ ] **Planned conformity route** Self-assessment, harmonised standard, or notified body — the route is chosen and resourced.

02

Build it secure

Essential security requirements for the product itself

Annex I, Part I — Essential requirements

The CRA's essential requirements for the **product** are set out in Annex I, Part I. These are not guidelines or best practices — they are mandatory legal requirements that every product with digital elements must meet before it is placed on the EU market. Non-conformance with these requirements is the primary basis on which market surveillance authorities can prohibit or withdraw a product and on which the European Commission can impose penalties of up to €15 million or 2.5% of global annual turnover.

The requirements are technology-neutral: they specify **what** security properties the product must have, not **how** to achieve them. Harmonised European Standards (hENs) being developed by CEN/CENELEC will describe accepted technical means of demonstrating conformity; until those standards are published (expected 2026–2027), manufacturers must document their own technical justification.

> **DESIGN-PHASE INTEGRATION**
>
> The essential requirements apply at the point the product is **placed on the market** — but meeting them after development is expensive and often impossible without re-architecture. Integrate security requirements into your product requirements document, threat model, and design review process from the earliest feasible stage. Retrofitting CE-marking compliance onto a shipped product is not a valid path.

Secure by design

The product must be **designed, developed, and produced** to ensure an appropriate level of cybersecurity based on the risks. This includes:

- Conducting a cybersecurity risk assessment during design and development (see Chapter 04 for the formal documentation requirement).
- Eliminating known exploitable vulnerabilities at time of placement on the market — not just patching them after the fact.
- Having security as a design goal, not an afterthought: threat modelling, attack surface analysis, and secure coding practices applied throughout development.

Secure by default

Products must be delivered in a **secure default configuration**. This is one of the most operationally significant requirements:

- **No default or generic passwords** — factory credentials must be unique per device or must require change on first use. Shared default passwords ("admin/admin") are prohibited.
- **Minimal attack surface** — only features and ports necessary for the product's intended use should be enabled by default. Everything else must be disabled.
- **Ability to reset to a secure state** — the product must support a factory reset or equivalent that returns it to a known-good, compliant security state, suitable for safe disposal or transfer to a new user.

Data protection built in

Products must protect the confidentiality, integrity, and availability of data they store, transmit, or process:

- Data at rest and in transit should be protected using appropriate cryptography (the CRA does not mandate specific algorithms — use current industry standards, e.g. AES-256, TLS 1.2+).
- The product must not process data beyond what is necessary for its intended functionality (data minimisation — aligned with GDPR Article 5).
- Personal data must be protected against unauthorised access, loss, or destruction.

Access control and resilience

- The product must implement **appropriate access control mechanisms** — authentication, authorisation, and where relevant, multi-factor authentication.
- Products must be **resilient** to denial-of-service attacks where this is relevant to their intended use.
- Cryptographic operations must use appropriate, up-to-date algorithms and key lengths — avoid deprecated ciphers (RC4, DES, MD5 for authentication, SHA-1 for signing).

> **LEGACY PRODUCT WARNING**
>
> If you have existing products that use hardcoded credentials, deprecated cryptography, or expose unnecessary attack surface, these must be remediated before the product is (re-)placed on the EU market after 11 December 2027. A product that is in production and unchanged before that date may continue to be sold only until the date the existing stock is exhausted — it cannot be replenished without compliance.

Security update capability

The product must **support security updates**. This means:

- The update mechanism itself must be secure (authenticated, integrity-checked — no unauthenticated over-the-air updates).
- Security updates must be delivered separately from functional updates so users can apply security patches without accepting new features.
- Updates must be available free of charge for the duration of the support period.
- Users must be **notified** of available security updates.

BUILD IT SECURE CHECKLIST

- [ ] **Threat model completed** Attack surface identified; threats rated by likelihood and impact.
- [ ] **No hardcoded or shared default credentials** Unique per-device credentials or forced change on first use.
- [ ] **Minimal attack surface by default** Unused ports, services, and interfaces disabled at ship.
- [ ] **Secure reset capability** Factory reset returns to a known-secure, documented state.

- [ ] **Data minimisation applied** Product collects and processes only what is necessary for intended function.
- [ ] **Encryption in use** Data at rest and in transit protected with current, non-deprecated algorithms.
- [ ] **Access control implemented** Authentication and authorisation in place; MFA available where relevant.
- [ ] **Secure update mechanism** OTA/remote updates are authenticated and integrity-checked.
- [ ] **Security updates are free and notified** Users receive notification of available patches; no paywall on security fixes.

03

Handle vulnerabilities

SBOM, CVD policy, and security updates across the support period

Annex I, Part II — Vulnerability handling requirements

The CRA does not stop at shipping a secure product. Annex I, Part II imposes ongoing obligations throughout the product's support period — the lifetime during which you must actively maintain its security posture. These obligations are some of the most operationally intensive in the regulation, because they require sustained processes and tooling, not just one-time engineering effort.

Software Bill of Materials (SBOM)

Every manufacturer must identify and document the **software components** of their product, including by drawing up a software bill of materials (SBOM). The CRA does not mandate a specific SBOM format, but the two dominant machine-readable standards — CycloneDX (OWASP) and SPDX (Linux Foundation/ISO 5962) — are explicitly referenced in guidance and are the practical choice.

At a minimum, the SBOM must cover top-level dependencies: the direct libraries, modules, and packages your product incorporates, plus their versions. Best practice is to extend this to transitive dependencies (your dependencies' dependencies) and to include:

- Component name, supplier, version
- Relationship type (depends on, contains, bundled)
- Hash / checksum for integrity verification
- License identifier (important for open-source compliance)

> **SBOM OPERATIONAL VALUE**
>
> An accurate SBOM is not just a compliance artefact — it is your primary tool for rapid triage when a new vulnerability (e.g. a new Log4Shell equivalent) is announced. Without it, determining whether your product is affected takes days; with it, a query takes minutes. Build the SBOM generation into your CI/CD pipeline using tools such as Syft, Trivy, or SPDX-Maven-Plugin — do not treat it as a documentation exercise done once at release.

Coordinated Vulnerability Disclosure (CVD) policy

Manufacturers must **establish and maintain a policy for coordinated vulnerability disclosure**. This policy must be publicly accessible (typically via a `security.txt` file at `/.well-known/security.txt` and linked from your product documentation) and must include:

- A **contact point** for receiving vulnerability reports from external researchers, customers, and national authorities. This can be an email address, a web form, or a dedicated security-reporting platform.
- An **acknowledgement process** — a commitment to acknowledge receipt of reports within a defined timeframe (industry norm: 2 business days).
- A **timeline commitment** — how long the manufacturer aims to remediate reported vulnerabilities before public disclosure (industry norm: 90 days, extendable by mutual agreement).
- Confirmation that the reporter will not face legal action for good-faith disclosure in accordance with the policy.

The CVD contact point must remain operational throughout the support period. If your organisation is acquired or wound down, the obligation to maintain this channel transfers to the new controller of the product.

TEMPLATE

CVD Policy — Minimum Elements

PUBLIC DISCLOSURE URL (SECURITY.TXT LOCATION) .....

VULNERABILITY REPORT CONTACT (EMAIL / FORM / PLATFORM) .....

ACKNOWLEDGEMENT SLA (E.G. 2 BUSINESS DAYS) .....

REMEDIATION TARGET TIMELINE (E.G. 90 DAYS) .....

SAFE HARBOUR / NON-RETALIATION STATEMENT REFERENCE .....

CVSS OR SEVERITY RATING METHODOLOGY USED .....

Register your CVD contact point with ENISA's vulnerability database (EUVD) once the registration process opens — expected H2 2026.

Security updates across the support period

The CRA requires manufacturers to **provide security updates for a period that reflects the expected use of the product** — but sets a floor: the support period must be **at least five years** from the date the product is placed on the market, unless the product's intended lifetime is shorter (which must be explicitly stated and justified in the technical documentation).

This has significant commercial implications:

- Manufacturers of low-cost IoT devices with short commercial lifecycles must now plan for a multi-year security maintenance programme.
- End-of-life announcements must give users sufficient notice to migrate or decommission.
- Where a manufacturer wishes to end support before five years, they must notify users and market surveillance authorities.

SUPPORT PERIOD PLANNING

Map your entire product portfolio against the five-year floor now. Products with low margins that currently receive only 12–18 months of software support may require either (a) a new commercial model to fund extended support, (b) architectural changes to reduce the cost of patching, or (c) a deliberate decision to withdraw them from the EU market before 11 December 2027.

Handling known vulnerabilities in shipped products

When a vulnerability is discovered (internally or reported externally) in a product already on the market:

1. Assess severity (CVSS score, exploitability, impact on CIA triad).
2. Develop and test a fix.
3. Release the security update promptly and notify users.
4. If the vulnerability is actively exploited, trigger the incident reporting process (Chapter 05).
5. Document the entire handling process in your vulnerability register.

VULNERABILITY HANDLING CHECKLIST

- [ ] **SBOM process in place** Machine-readable SBOM (CycloneDX or SPDX) generated at each release.
- [ ] **SBOM covers top-level dependencies** All direct libraries/modules with name, version, and hash documented.
- [ ] **CVD policy published** Publicly accessible via security.txt and product documentation.
- [ ] **Vulnerability contact point operational** Monitored inbox or form; acknowledgement SLA defined and staffed.
- [ ] **Support period defined per product** At least 5 years documented; shorter periods explicitly justified.
- [ ] **Patch release process documented** From vulnerability triage to user notification — steps, owners, SLAs.
- [ ] **Vulnerability register maintained** Internal log of discovered vulnerabilities, severity, fix timeline, and outcome.

04

Prove conformity

Risk assessment, technical documentation, CE marking

From compliant to provably compliant

Building a secure product is necessary but not sufficient. The CRA requires manufacturers to **demonstrate** conformity through a structured set of documentation and procedural steps. This is the machinery of EU product regulation applied to cybersecurity: a risk assessment, a dossier of technical evidence, a formal conformity assessment, a signed Declaration of Conformity, and the CE marking affixed to the product.

Market surveillance authorities can demand access to any part of this evidence chain at any time. Technical documentation must be maintained for **ten years** from the date the product is placed on the market or the end of the support period — whichever is later.

Cybersecurity risk assessment (Article 13)

Every manufacturer must carry out a **cybersecurity risk assessment** of the product during the design and development phase — and update it when changes affect the product's security properties. This assessment must:

- Identify and analyse the cybersecurity risks associated with the product's intended use and foreseeable misuse.
- Consider the product's interaction with its environment (network, users, other devices).
- Document the threats and the controls implemented to mitigate them.
- Inform the design choices documented elsewhere in the technical file.

The risk assessment is not a one-time exercise: it must be reviewed when the product is substantially modified, when new vulnerabilities are identified in components, and when the threat landscape changes significantly.

> **RISK ASSESSMENT METHODOLOGIES**
>
> The CRA does not mandate a specific methodology. Widely accepted approaches include: STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege), PASTA, TARA (Threat Analysis and Risk Assessment — common in automotive/industrial), and IEC 62443-3-2 for industrial systems. ENISA publishes guidance on asset identification and risk assessment approaches that are accepted by market surveillance authorities.

Technical documentation (Annex VII)

The technical documentation must provide authorities with everything they need to assess conformity. Annex VII specifies the required contents:

- General description of the product (intended use, hardware/software components, versions)
- The cybersecurity risk assessment
- Design and development documentation: architecture diagrams, data flow diagrams, key design decisions and their security rationale
- The SBOM
- Secure development lifecycle documentation: processes, tools, testing evidence
- Vulnerability handling and disclosure procedures
- List of harmonised standards applied (when published), or alternative technical justification
- EU Declaration of Conformity (copy)
- For IoT/hardware: circuit diagrams, PCB layouts where relevant

TEN-YEAR RETENTION

Technical documentation must be kept for at least ten years from the date of last placement on the market or the end of the support period — whichever is later. For a product first sold in December 2027 with a five-year support period, that means retention until at least 2042. Build your document management and archiving strategy with this in mind.

Conformity assessment route by tier

1. **Default class**

   Use the internal control procedure (Module A). Manufacturer conducts its own assessment, draws up technical documentation, signs the EU Declaration of Conformity, and affixes CE marking.

2. **Important Class I**

   Apply a harmonised European Standard (when available). If no relevant hEN is available, use EU-type examination by a notified body (Module B) or EU-type examination followed by conformity to type (Module C).

3. **Important Class II**

   Mandatory notified body involvement. Use EU-type examination (Module B) + conformity to type (Module C), or full quality assurance (Module H). A notified body must be engaged.

4. **Critical (Annex IV)**

   Notified body assessment required. Where an EU cybersecurity certificate is available under the EU Cybersecurity Act (EUCS) scheme for that product category, the certificate may be used. If not yet available, full notified body assessment applies.

EU Declaration of Conformity (Annex V)

The EU Declaration of Conformity (DoC) is the formal statement that the product meets the CRA's essential requirements. It must:

- Identify the product (name, type, model, serial/batch/version number)
- Name and address of the manufacturer (and authorised representative if applicable)
- State that the declaration is issued under the sole responsibility of the manufacturer
- Reference the regulation: "Regulation (EU) 2024/2847"
- List the harmonised standards or technical specifications applied, or reference the notified body and its opinion number (for Class II/Critical)
- Be signed, dated, and identified by the signatory's name and function
- Accompany the product or be available online, with a QR code or URL on the product or packaging

Affixing CE marking

Once the DoC is signed, the CE marking must be affixed to the product — or, where this is not physically possible (e.g. certain software), to the packaging, accompanying documents, or via a digital certificate. The marking must be visible, legible, and indelible. For Class II and Critical products, the four-digit number of the notified body involved must be affixed alongside the CE mark.

PROVE CONFORMITY CHECKLIST

- [ ] **Cybersecurity risk assessment completed** Threats identified, controls mapped, residual risk accepted — for each in-scope PDE.
- [ ] **Technical documentation file created** Annex VII elements assembled and version-controlled.
- [ ] **Conformity assessment route confirmed** Correct module selected for each product's class; notified body engaged if required.
- [ ] **EU Declaration of Conformity drafted** Annex V requirements met; signed by authorised person.
- [ ] **CE marking affixed** Visible and legible on product, packaging, or digital certificate.
- [ ] **Documentation retention plan in place** 10-year retention policy and storage infrastructure confirmed.

05

Reporting readiness

The new 24/72/14-day incident and vulnerability reporting cycle

A new obligation: mandatory reporting to ENISA

From **11 September 2026**, manufacturers must notify ENISA — via its Single Reporting Platform (SRP) — whenever they become aware of either:

- An **actively exploited vulnerability** in their product (a vulnerability for which there is credible evidence of exploitation in the wild, regardless of whether your specific product has been compromised).
- A **severe incident** affecting the security of the product that could impact a significant number of users or critical infrastructure.

This obligation is separate from the GDPR data breach notification obligation (which goes to supervisory authorities and is triggered by personal data compromise). CRA reporting is specifically about product security, and it goes to ENISA and the national CSIRT simultaneously.

> **REPORTING IS LIVE FROM 11 SEP 2026 — BEFORE FULL PRODUCT COMPLIANCE**
>
> The reporting obligation applies from 11 September 2026, a full 15 months before the product-compliance deadline of 11 December 2027. This means that even if your product is not yet fully CRA-compliant, you must have reporting processes and SRP access in place by September 2026 if your products are on the EU market.

The reporting timeline

The CRA sets a three-stage notification process, mirroring NIS2's incident reporting model but applied to product security:

1. **Early warning — within 24 hours**

   Notify ENISA that you are aware of an actively exploited vulnerability or severe incident. This is a minimal notification: product identifier, nature of the issue, and whether you believe critical infrastructure or significant user numbers are at risk. The clock starts when you first become *aware*, not when you have completed your investigation.

2. **Detailed notification — within 72 hours**

   Provide a more complete picture: initial assessment of severity and impact, known affected versions, current status of your investigation, and any interim mitigations or workarounds you can share publicly. The 72-hour clock also runs from first awareness.

3. **Final report — within 14 days (one month for severe incidents)**

   Submit the complete technical account: root cause analysis, full list of affected products/versions, remediation actions taken (patch released, advisory published), and steps taken to prevent recurrence. For severe incidents, the deadline is one month from initial awareness.

Know your national CSIRT

Each EU Member State designates one or more Computer Security Incident Response Teams (CSIRTs) under NIS2. For CRA reporting, your **national CSIRT** is the authority that receives your notifications via the SRP and may follow up with technical support or investigations. Identify the

CSIRT(s) for the Member States where your company is established and where your most significant user base operates.

Key national CSIRTs include: BSI (Germany), ANSSI (France), NCSC-NL (Netherlands), CERT.be (Belgium), NCSC-UK (note: UK is post-Brexit, but often co-operates), and CERT-EU for EU institutions. ENISA maintains the full list at enisa.europa.eu.

SINGLE REPORTING PLATFORM (SRP)

ENISA is building the SRP as the central intake for all CRA notifications. Registration procedures and the API specification for automated reporting are expected to be published by ENISA in 2025–2026. Monitor enisa.europa.eu/topics/cra for updates and register your organisation as early as registration opens — do not leave this to the week before the September 2026 deadline.

Rehearse the playbook

Regulatory reporting under time pressure is high-stakes: a missed 24-hour window is a compliance failure, and an inaccurate report can expose you to enforcement action. The only way to be ready is to have a tested playbook:

- **Define trigger criteria:** what observable evidence constitutes “awareness” of an actively exploited vulnerability? (E.g.: a CISA KEV listing, a CVE with weaponised PoC, a researcher report with attached exploit, customer evidence of exploitation.)
- **Assign roles:** who makes the call to trigger reporting? Who drafts the notification? Who has authority to sign and submit? Who is the ENISA SRP account holder?
- **Document escalation paths:** out-of-hours and holiday coverage; who is the backup for each role?
- **Run a tabletop exercise:** simulate receipt of a “your product is being actively exploited” alert at 11pm on a Friday, and walk through the process of submitting the 24-hour early warning before the deadline.

HANDS-ON · 2 HOURS

Tabletop exercise: incident reporting drill. Schedule a 2-hour session with your security, legal, and communications leads. Use this scenario: a security researcher contacts your CVD inbox at 14:00 on a Monday attaching a working exploit for a critical authentication bypass in your flagship product. The exploit is already posted to a dark-web forum. Walk through: (1) confirming “awareness” has been triggered, (2) who notifies whom internally, (3) drafting and submitting the 24-hour early warning to the ENISA SRP, (4) drafting the 72-hour detailed notification, (5) preparing the public advisory. Identify every gap in your process and assign owners.

REPORTING READINESS CHECKLIST

- [ ] **SRP account registered** ENISA Single Reporting Platform access established and tested before 11 Sep 2026.

- [ ] **National CSIRT(s) identified** Primary CSIRT contact for your establishment and major markets logged.
- [ ] **Reporting trigger criteria defined** Clear, written definition of what constitutes 'awareness' of an exploitable vulnerability or severe incident.
- [ ] **Reporting roles and escalation documented** Named owners for 24h, 72h, and final report; out-of-hours coverage assigned.
- [ ] **Notification templates prepared** Draft templates for 24h early warning and 72h detailed notification ready to complete quickly.
- [ ] **Tabletop exercise completed** At least one rehearsal of the full reporting cycle conducted before Sep 2026 go-live.
- [ ] **CRA reporting distinguished from GDPR breach reporting** Teams understand that CRA reports go to ENISA/CSIRT, not just the data protection authority.

06

Master checklist & next steps

Consolidated sign-off and your CRA Facts resources

The consolidated CRA readiness checklist

Use this master checklist for your final readiness review and for sign-off by your compliance lead or legal counsel. Each item maps to a detailed chapter above. This is a summary — refer back to the chapter checklists for the full sub-item detail.

SCOPE & ROLES

- [ ] **Role confirmed** Manufacturer, importer, distributor, or open-source steward — documented.
- [ ] **Product inventory complete** All hardware, software, and firmware placed on the EU market catalogued.
- [ ] **Exclusions verified** MDR, IVDR, automotive, aviation, and marine carve-outs checked per product.
- [ ] **CRA class assigned per product** Default / Important Class I / Important Class II / Critical — recorded in product register.
- [ ] **Conformity route selected** Self-assessment or notified body engagement — resourced and scheduled.

PRODUCT SECURITY (ANNEX I, PART I)

- [ ] **Threat model completed for each PDE** Attack surface documented; STRIDE or equivalent methodology applied.
- [ ] **No hardcoded or shared default credentials** Per-device unique credentials or mandatory first-use change implemented.
- [ ] **Minimal attack surface by default** Unused ports, services, protocols disabled at factory settings.
- [ ] **Secure reset to known-good state** Factory reset procedure documented and tested.
- [ ] **Data minimisation applied** Product collects only what is required for intended function.
- [ ] **Encryption in use** Data at rest and in transit: current, non-deprecated algorithms; no RC4, DES, MD5 for auth.
- [ ] **Access control implemented** Authentication, authorisation, MFA where relevant — across all product interfaces.
- [ ] **Secure, authenticated update mechanism** OTA/remote updates integrity-checked and authenticated.

- [ ] **Security updates free and notified to users** No paywall on security patches; users notified of available updates.

VULNERABILITY HANDLING (ANNEX I, PART II)

- [ ] **SBOM generated per release** Machine-readable CycloneDX or SPDX; at minimum all top-level dependencies.
- [ ] **CVD policy published** Publicly accessible; contact point, acknowledgement SLA, timeline, safe harbour.
- [ ] **Vulnerability contact point staffed** Monitored continuously; backup coverage documented.
- [ ] **Support period ≥ 5 years documented per product** Or shorter period explicitly justified and stated.
- [ ] **Vulnerability register and patch process in place** Triage → fix → release → user notification: steps, owners, SLAs.

CONFORMITY DOCUMENTATION

- [ ] **Cybersecurity risk assessment completed** Per product; updated when design changes or new threats emerge.
- [ ] **Technical documentation file complete** All Annex VII elements assembled, version-controlled, accessible.
- [ ] **EU Declaration of Conformity signed** Annex V requirements met; signed by authorised signatory.
- [ ] **CE marking affixed** Visible, legible, and indelible on product, packaging, or digital certificate.
- [ ] **10-year retention plan active** Document management system configured for minimum retention period.

REPORTING (LIVE 11 SEP 2026)

- [ ] **ENISA SRP account registered and tested** Before 11 September 2026.
- [ ] **National CSIRT(s) identified and contacts logged**
- [ ] **Reporting playbook documented** Trigger criteria, roles, escalation, out-of-hours coverage.

- [ ] **Notification templates ready** 24h early warning and 72h detailed notification templates drafted.
- [ ] **Tabletop exercise completed** Full reporting cycle rehearsed with security, legal, and comms.

STAY CURRENT — THE CRA IS STILL EVOLVING

Get The CRA Brief

The CRA's implementing acts, delegated regulations, harmonised standards, and ENISA guidance are still being published. The landscape will look different in six months. Subscribe to **The CRA Brief** — our free newsletter — to get plain-English summaries of every material development: new guidance, standard adoptions, enforcement actions, and deadline changes.

→ Access the free interactive version of this checklist

→ Free tools, templates, and updates at cra-facts.com

QUICK NAVIGATION

Jump to any chapter

Click a tile to go directly to that section.

Interactive checklist →

Visit cra-facts.com →

CRA Facts

CRA compliance is a process, not a *one-time audit.*

Free tools, templates, and expert briefings at
cra-facts.com