EVERYTHING ANNEX VII EXPECTS

Your CRA technical file, *mapped out.*

A section-by-section index of the technical documentation Annex VII requires, plus a fill-in EU Declaration of Conformity outline — so you can assemble a complete, compliant technical file.

This document is a practical reference for compliance owners, product managers, and legal teams preparing the technical documentation required under the EU Cyber Resilience Act (Regulation (EU) 2024/2847). It maps every section Annex VII expects onto a structured, fill-in index, and provides a parallel EU Declaration of Conformity outline you can draft alongside it. Use it as a working checklist from first article-review through to CE marking.

Guidance, not legal advice. *This index is an educational reference. It does not constitute legal advice and does not replace the obligation to read Regulation (EU) 2024/2847 and any guidance issued by the European Commission or relevant national authorities. Consult qualified legal counsel for your specific product and market situation.*

CONTENTS

00

What the technical documentation is

Why it exists, what it proves, and who can ask to see it.

The technical file: *your evidence dossier*

Before a product with digital elements can carry the CE mark under the EU Cyber Resilience Act, a manufacturer must draw up a technical documentation file. This is not a marketing document. It is the structured evidence package that demonstrates — to market surveillance authorities, notified bodies, and ultimately the public — that the product was designed, developed, and produced to meet the essential cybersecurity requirements in Annex I of the CRA.

Article 31 of the CRA places the obligation squarely on the manufacturer: the documentation must be **drawn up before placing on the market**, must be **kept up to date** as the product changes, must be **retained for at least ten years** after the last unit is placed on the market (or the support period if longer), and must be **made available on request** to any market surveillance authority in any Member State.

> **LEGAL ANCHOR: ART. 31 + ANNEX VII**
>
> **Article 31** requires manufacturers to draw up technical documentation before placing a product with digital elements on the market. **Annex VII** specifies the nine categories of content that documentation must contain. Reading the two together gives you the complete obligation — Annex VII is the detailed checklist that fleshes out what Art. 31 demands.

The role of the technical file in conformity assessment

The technical documentation serves three interconnected purposes:

1. Conformity assessment input. When you choose a conformity assessment route — self-assessment for Class I products, third-party assessment by an EU-notified body for Class II and critical products — the technical file is the primary input. The assessor (internal or external) works through it to conclude that Annex I essential requirements are met.

2. EU Declaration of Conformity support. When you sign and issue the EU Declaration of Conformity (DoC) under Annex V, you are attesting that you have the evidence to back up the declaration. The technical documentation **is** that evidence. The DoC references the standards and specifications you applied; the technical file contains the records showing how you applied them.

3. Post-market surveillance. Market surveillance authorities can demand the technical file at any time. If a vulnerability or incident occurs after market placement, the file is the record used to assess whether the manufacturer fulfilled their obligations. An incomplete or out-of-date file is itself a non-compliance.

Who is responsible

The obligation rests on the **manufacturer** — the legal or natural person who places a product under their own name or trademark, or who modifies a product materially enough to bring it back into scope. Importers and distributors have their own CRA obligations, but the technical file is a manufacturer obligation. If you outsource development, you remain the responsible party: you must ensure the documentation is complete and that you can access and maintain it.

OPEN-SOURCE MAINTAINERS

If you make available a product with digital elements in the course of a commercial activity — even an open-source one — you may be treated as the manufacturer for CRA purposes. The technical documentation obligation follows you, not only the company that packages your code downstream. Check the Commission guidance on the open-source carve-out carefully if this applies to you.

How the file relates to CE marking

CE marking is the outward signal that conformity assessment is complete. The sequence is: draw up the technical documentation → conduct conformity assessment → issue the EU Declaration of Conformity → affix the CE mark. You cannot lawfully affix CE until all prior steps are complete and the technical documentation is in order. The mark is not a self-declaration of quality; it is a legal statement that the conformity process was followed.

CHAPTER 00 CHECKLIST

- [ ] **Understand the legal basis** Art. 31 + Annex VII of Regulation (EU) 2024/2847 identified and bookmarked.
- [ ] **Identify the responsible manufacturer** The legal entity that will sign the DoC and maintain the technical file is confirmed.
- [ ] **Confirm product class** Class I (self-assess), Class II (notified body), or critical product — determines conformity assessment route.
- [ ] **Set a file retention calendar** 10-year retention (or support period if longer) tracked from last unit placed on market.
- [ ] **Assign a file owner** One named person in the organisation owns completeness and currency of the technical file.

01

The technical documentation index

A fill-in template of every section Annex VII expects.

Section-by-section: *the nine Annex VII areas*

Annex VII of the CRA structures the technical documentation into nine content areas. The template below maps each area to the documents, records, and artefacts you need to produce or reference. Fill in the bracketed fields and use the checklist at the end of each section to verify completeness before you move to conformity assessment.

Every entry in this index should be a **live pointer** — either a document stored in your file system with a version number and date, or a direct statement of the fact (for short items). The index itself becomes the cover sheet of your technical file package.

> **VERSIONING CONVENTION**
>
> Date each document in ISO 8601 format (YYYY-MM-DD). Use semantic versioning (MAJOR.MINOR.PATCH) for the product and for any document that tracks the product version. When the product changes in a way that affects a CRA essential requirement, the corresponding section of the technical documentation must be updated and a new version issued before the updated product ships.

Section 1 — General description of the product

This section gives market surveillance authorities the factual baseline: what the product is, who it is for, and what it does. It is not a data sheet; it is a plain-language, technically complete account that a non-specialist engineer at a national authority can understand.

TEMPLATE

Section 1 — General description

PRODUCT NAME & TRADE NAME .....

MANUFACTURER NAME & REGISTERED ADDRESS .....

EU AUTHORISED REPRESENTATIVE (IF APPLICABLE) .....

INTENDED PURPOSE — PLAIN LANGUAGE, ONE PARAGRAPH .....

PRODUCT CATEGORY (AS PER ANNEX III / CRA CLASS) .....

PRODUCT TYPES / CONFIGURATIONS / SKUS COVERED BY THIS FILE .....

HARDWARE VERSION(S) IN SCOPE .....

FIRMWARE / SOFTWARE VERSION(S) IN SCOPE .....

HOW THE PRODUCT WORKS — FUNCTIONAL OVERVIEW (≤ 1 PAGE) .....

NETWORK INTERFACES AND CONNECTIVITY (LIST ALL) .....

DATA PROCESSED AND STORED BY THE PRODUCT .....

REFERENCE TO PHOTOS, DIAGRAMS, OR RENDERS (DOC ID) .....

REFERENCE TO USER DOCUMENTATION (DOC ID) .....

Attach or reference: exploded diagrams, interface schematics, data-flow diagrams.

- [ ] **General description complete** All configured variants and software versions covered.
- [ ] **Photos / diagrams referenced** At least one labelled diagram showing major components and interfaces.

- [ ] **Data flows documented** What data enters, leaves, and persists on the device is explicitly stated.

Section 2 — Design, development & production

This section documents **how** the product was built. For a software-only product this means the secure development lifecycle, the build environment, and release pipeline. For hardware-software combinations it also includes hardware design records. Where applicable — particularly for products processed as safety-critical or highly sensitive — this section must include evidence of the secure development process used.

TEMPLATE

Section 2 — Design, development & production

DEVELOPMENT METHODOLOGY (E.G. AGILE, SDL, ISO/IEC 27034 REF) .....

SECURE DEVELOPMENT LIFECYCLE STANDARD APPLIED (DOC ID) .....

THREAT MODELLING RECORDS (DOC ID, VERSION, DATE) .....

ARCHITECTURE DESIGN DOCUMENTS (DOC ID) .....

HARDWARE DESIGN RECORDS, IF APPLICABLE (DOC ID) .....

SOURCE-CODE MANAGEMENT SYSTEM AND BRANCH-PROTECTION POLICY .....

BUILD ENVIRONMENT DESCRIPTION (REPRODUCIBLE BUILD? Y/N) .....

CI/CD PIPELINE — SECURITY GATES APPLIED (DOC ID) .....

STATIC ANALYSIS / SAST TOOL(S) USED AND FINDINGS LOG (DOC ID) .....

DYNAMIC ANALYSIS / DAST / FUZZING RESULTS (DOC ID) .....

PENETRATION TEST REPORT(S), IF CONDUCTED (DOC ID, TESTER NAME) .....

PRODUCTION QA PROCESS FOR HARDWARE, IF APPLICABLE (DOC ID) .....

Tip: Reference documents by ID rather than embedding them. The index is the map; the documents are the territory.

- [ ] **SDL process documented** The secure development lifecycle is described or referenced.
- [ ] **Threat model in file** At least one threat model covering the current product version.

- [ ] **Security testing evidence** SAST/DAST outputs, pen-test reports, or equivalent, with disposition of findings.

Section 3 — Cybersecurity risk assessment (Art. 13)

Article 13(2) requires the manufacturer to undertake a cybersecurity risk assessment and integrate its results into the design. The technical file must contain that assessment — not a summary, but the actual assessment or a direct reference to a versioned document containing it. The assessment must cover the product's entire lifecycle, including the support period.

TEMPLATE

Section 3 — Cybersecurity risk assessment

RISK ASSESSMENT METHODOLOGY (E.G. STRIDE, PASTA, ISO 27005) .....

RISK ASSESSMENT DOCUMENT (DOC ID, VERSION, DATE) .....

THREAT ACTORS AND ATTACK SURFACES IDENTIFIED .....

RISK SCENARIOS WITH LIKELIHOOD AND IMPACT RATINGS .....

MITIGATIONS ADOPTED — MAPPED TO ANNEX I REQUIREMENTS .....

RESIDUAL RISKS ACCEPTED — RATIONALE DOCUMENTED .....

REVIEW TRIGGER: WHEN WILL ASSESSMENT BE UPDATED? .....

DATE OF LAST REVIEW / UPDATE .....

The risk assessment is a living document. Record the review date and the trigger condition (e.g. major version release, new CVE in a dependency, change in deployment context).

RISK ASSESSMENT SCOPE

The CRA risk assessment must cover the **entire lifecycle**, including the period after sale when the product is in the hands of the user. Consider update delivery mechanisms, end-of-support scenarios, and the risk introduced by the product's typical deployment context — not just the product in isolation.

- [ ] **Risk assessment document referenced** Versioned, dated document in the technical file.

- [ ] **Annex I mapping complete** Each identified risk mitigation maps to one or more Annex I essential requirements.
- [ ] **Lifecycle scope confirmed** Assessment covers the full stated support period.

Section 4 — Essential requirements — how each is met

This is often the largest section of the technical file. For every essential requirement in Annex I, Parts I and II, you must state: (a) whether the requirement applies to your product, (b) if it applies, how you meet it — by reference to harmonised standards, common specifications, cybersecurity certification schemes under Regulation (EU) 2019/881, or other technical solutions, and (c) where the evidence lives in the file.

TEMPLATE

Section 4 — Essential requirements mapping

HARMONISED STANDARD(S) APPLIED (EN/ISO NUMBER, VERSION, DATE OF PUBLICATION IN OJ) ....

COMMON SPECIFICATION(S) APPLIED (COMMISSION IMPLEMENTING REGULATION REF) ....

EU CYBERSECURITY CERTIFICATION APPLIED (SCHEME, CERTIFICATE NUMBER) ....

OTHER TECHNICAL SOLUTIONS FOR REQUIREMENTS NOT COVERED BY ABOVE ....

For each Annex I, Part I requirement — record below:

REQ 1 — NO KNOWN EXPLOITABLE VULNERABILITIES: EVIDENCE REFERENCE ....

REQ 2 — SECURE BY DEFAULT CONFIGURATION: EVIDENCE REFERENCE ....

REQ 3 — PROTECTION OF CONFIDENTIALITY: EVIDENCE REFERENCE ....

REQ 4 — PROTECTION OF INTEGRITY: EVIDENCE REFERENCE ....

REQ 5 — PROCESSING ONLY NECESSARY DATA: EVIDENCE REFERENCE ....

REQ 6 — PROTECTION OF AVAILABILITY: EVIDENCE REFERENCE ....

REQ 7 — MINIMISING ATTACK SURFACE: EVIDENCE REFERENCE ....

REQ 8 — REDUCED IMPACT OF SECURITY INCIDENTS: EVIDENCE REFERENCE ....

REQ 9 — SECURITY UPDATES [illegible] EVIDENCE REFERENCE ....

PART II, REQ 5 — CVD POLICY: [illegible] EVIDENCE REF ....

PART II REQ 1 — IDENTIFY AND DOCUMENT VULNERABILITIES AND COMPONENTS: EVIDENCE REF

For each Annex I, Part II (vulnerability handling) requirement:

[illegible] requirement your product genuinely cannot trigger. Document the reasoning; do not leave it blank.

- [ ] **All Annex I Part I requirements addressed** Each requirement either evidenced or formally marked N/A with rationale.
- [ ] **All Annex I Part II requirements addressed** Vulnerability handling requirements covered.
- [ ] **Standards / specifications listed** OJ publication dates recorded for harmonised standards; implementing regulation references for common specifications.

Section 5 — Software bill of materials (SBOM)

The CRA requires manufacturers to identify and document components in the product — effectively mandating an SBOM. The SBOM must cover all third-party software components, including open-source dependencies. It is a critical input to your vulnerability management process: you cannot monitor for CVEs in components you have not identified.

TEMPLATE

Section 5 — SBOM

SBOM DOCUMENT (DOC ID, VERSION, DATE, MACHINE-READABLE FORMAT) .....

SBOM STANDARD APPLIED (E.G. SPDX 2.3, CYCLONEDX 1.6) .....

SBOM GENERATION TOOL(S) AND PIPELINE INTEGRATION .....

FIRST-PARTY COMPONENTS LISTED .....

THIRD-PARTY / OPEN-SOURCE COMPONENTS LISTED (COUNT) .....

TRANSITIVE DEPENDENCY DEPTH COVERED .....

PROCESS FOR KEEPING SBOM CURRENT ON EACH RELEASE .....

MINIMUM FIELDS CAPTURED PER COMPONENT (NAME, VERSION, SUPPLIER, LICENCE, HASH) .....

The SBOM is a living document. It must be updated at each release that changes the component set. Consider publishing a subset of the SBOM for users on request (Annex I Part II).

MINIMUM SBOM FIELDS

What the CRA implies

Component name, version, supplier, licence identifier, cryptographic hash. Enough to look up a CVE and know if you are affected.

RECOMMENDED SBOM FORMAT

SPDX or CycloneDX

Both are tooling-supported, machine-readable, and widely accepted by regulators and customers. CycloneDX has richer vulnerability extension support.

- [ ] **SBOM generated and in file** Machine-readable file (SPDX or CycloneDX) referenced by doc ID.
- [ ] **Transitive dependencies covered** Not just direct dependencies — recursive dependency tree captured.
- [ ] **SBOM update process documented** Clear owner and trigger condition for SBOM refresh.

Section 6 — Vulnerability handling

This section documents your process for identifying, triaging, remediating, and disclosing vulnerabilities across the product's support period. It must include your coordinated vulnerability disclosure (CVD) policy, your communication channels for researchers and users, and the process by which security updates reach end users.

TEMPLATE

Section 6 — Vulnerability handling

VULNERABILITY MANAGEMENT PROCESS DOCUMENT (DOC ID) .....

CVD POLICY — URL AND/OR DOCUMENT REFERENCE .....

SECURITY.TXT FILE URL (WHERE HOSTED) .....

CONTACT CHANNEL FOR SECURITY RESEARCHERS .....

INTERNAL TRIAGE SLA (E.G. CRITICAL: 24H ACKNOWLEDGE, 72H TRIAGE) .....

PATCH RELEASE PROCESS (DOC ID) .....

SECURITY UPDATE DELIVERY MECHANISM FOR END USERS .....

UPDATE SIGNING / INTEGRITY VERIFICATION METHOD .....

ENISA EUVD / EU COORDINATED DISCLOSURE PROCESS REFERENCE .....

PROCESS FOR NOTIFYING USERS OF ACTIVELY EXPLOITED VULNERABILITIES .....

Annex I Part II requires a CVD policy to be in place before placing on market. Do not leave this to post-launch.

- [ ] **CVD policy published** Accessible to external researchers before product ships.
- [ ] **Security update delivery tested** Update mechanism verified to reach end-user devices in normal operating conditions.
- [ ] **ENISA notification process mapped** Responsibilities assigned for reporting actively exploited vulnerabilities within 24-hour window.

Section 7 — Support period

The CRA requires the manufacturer to state the support period — the duration for which the product will receive security updates — and to make this information available to users. The support period must reflect the expected use lifetime of the product. The Commission has indicated a presumed minimum of five years unless the expected lifetime is shorter.

TEMPLATE

Section 7 — Support period

STATED SUPPORT PERIOD (YEARS FROM DATE OF MARKET PLACEMENT) .....

EXPECTED END-OF-SUPPORT DATE (OR FORMULA, E.G. 5 YEARS FROM LAST UNIT SHIPPED) .....

RATIONALE FOR STATED DURATION .....

WHERE THE SUPPORT PERIOD IS DISCLOSED TO USERS (URL / LABEL / DOCUMENTATION) .....

PROCESS FOR NOTIFYING USERS OF END-OF-SUPPORT .....

WHAT HAPPENS TO SECURITY UPDATES WHEN SUPPORT ENDS .....

If a shorter period than 5 years is claimed, the technical file must contain clear justification based on product lifetime. Regulators will scrutinise short support periods for high-use consumer products.

- [ ] **Support period stated and documented** Specific date or deterministic formula, not a vague policy statement.
- [ ] **User-facing disclosure in place** Users can find the end-of-support date before purchase.
- [ ] **Rationale recorded** Technical file contains the reasoning for the chosen duration.

Section 8 — EU Declaration of Conformity

The technical file must contain a copy of the signed EU Declaration of Conformity (or a reference to where it is held). See Chapter 02 of this guide for the full DoC template. In the index, record the document reference and the date it was signed.

TEMPLATE

Section 8 — EU Declaration of Conformity reference

DOC DOCUMENT ID .....

DATE OF ISSUE .....

SIGNATORY NAME AND FUNCTION .....

LOCATION OF SIGNED ORIGINAL (FILE PATH / ARCHIVE SYSTEM) .....

URL WHERE DOC IS PUBLICLY AVAILABLE (IF APPLICABLE) .....

The DoC must be available to market surveillance authorities on request and, under the CRA, may need to be accessible to users. Keep a signed PDF in your technical file archive.

- [ ] **DoC signed and archived** Wet or qualified electronic signature. PDF/A format recommended.
- [ ] **DoC references correct harmonised standards** Same standards listed in Section 4 of this index.

Section 9 — Notified body reports and certificates (Class II / critical)

For Class II and critical products, conformity assessment involves a EU-notified body. The technical file must contain the relevant examination or audit reports, and the certificates issued. For Class I products assessed by self-declaration, this section records that self-assessment was the route used.

TEMPLATE

Section 9 — Notified body records

CONFORMITY ASSESSMENT ROUTE (SELF-ASSESSMENT / NB TYPE-EXAMINATION / NB AUDIT) .....

NOTIFIED BODY NAME (IF USED) .....

NOTIFIED BODY EU REGISTRATION NUMBER (IF USED) .....

EXAMINATION / ASSESSMENT REPORT (DOC ID, DATE) .....

CERTIFICATE NUMBER AND EXPIRY (IF ISSUED) .....

CONDITIONS OR OBSERVATIONS FROM NB (DOC ID) .....

For Class I self-assessment: record the date of assessment, the person(s) responsible, and the internal review record used. This is still required in the technical file even though no NB is involved.

- [ ] **Conformity assessment route confirmed** Product class and chosen route formally recorded.
- [ ] **NB certificate in file (if applicable)** Current certificate with expiry date tracked.

02

EU Declaration of Conformity outline

A fill-in DoC template aligned to Annex V of the CRA.

The Declaration: *your legal attestation*

The EU Declaration of Conformity (DoC) is the formal document in which the manufacturer attests — under sole legal responsibility — that the product meets the essential requirements of the CRA and any other applicable Union legislation. It is required by Article 28 and must follow the structure set out in Annex V. Without it, the CE mark cannot lawfully be affixed.

The DoC is a relatively short document, but every field matters. An incomplete or incorrectly structured DoC is a non-compliance in its own right. The template below maps directly to the Annex V requirements.

> **ANNEX V STRUCTURE**
>
> Annex V of Regulation (EU) 2024/2847 specifies the required content of the EU Declaration of Conformity. The declaration must contain all elements listed in Annex V, must be drawn up in one of the official languages of the Member States where the product is made available, and must be kept available for ten years after the last unit is placed on the market.

Completing the DoC

The Declaration must be signed by a natural person with authority to represent the manufacturer — typically a director, chief compliance officer, or an explicitly authorised technical signatory. The signatory must be identified by name and function in the document.

TEMPLATE

EU Declaration of Conformity — Annex V

DOC REFERENCE NUMBER .....

1. Manufacturer

MANUFACTURER NAME .....

MANUFACTURER REGISTERED ADDRESS (STREET, CITY, POSTCODE, COUNTRY) .....

EU AUTHORISED REPRESENTATIVE NAME & ADDRESS (IF MANUFACTURER OUTSIDE EU) .....

2. Statement of responsibility

"THIS DECLARATION OF CONFORMITY IS ISSUED UNDER THE SOLE RESPONSIBILITY OF THE MANUFACTURER." .....

3. Object of the declaration

PRODUCT NAME AND TRADE NAME .....

PRODUCT TYPE / MODEL IDENTIFIER .....

BATCH OR SERIAL NUMBER (OR REFERENCE TO LABELLING) .....

SOFTWARE / FIRMWARE VERSION(S) COVERED .....

INTENDED PURPOSE (BRIEF) .....

4. Statement of conformity

"THE OBJECT DESCRIBED ABOVE IS IN CONFORMITY WITH REGULATION (EU) 2024/2847 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL ON HORIZONTAL CYBERSECURITY REQUIREMENTS FOR PRODUCTS WITH DIGITAL ELEMENTS." .....

REFERENCES TO ANY OTHER [illegible] .....

6. Signed by (and capacity)

The DoC must be translated into the official language(s) of each Member State where the product is made available. Keep one master (usually English) and track translations.

Language and translation obligations

If you place your product in multiple EU markets, the DoC must be available in the official language of each Member State on request — and in some cases by default. Many manufacturers issue the DoC in English plus German and French as a minimum, then translate further based on distribution.

Machine translation is not recommended for legal documents. Use a qualified technical translator for each language version, and version-control translations alongside the source document.

> **TRANSLATION VERSION CONTROL**
>
> When you update the DoC (new product version, new standard applied, new notified body), every translated version must also be updated. A translation that refers to a superseded standard is itself a non-compliance. Track translation status in the same document management system as the source.

CHAPTER 02 CHECKLIST

- [ ] **DoC drafted to Annex V structure** All seven Annex V elements present in the document.
- [ ] **Standards correctly referenced** Same standards as in the technical file Section 4; OJ publication dates included.
- [ ] **Signatory authorised** Signatory has formal authority to bind the manufacturer.
- [ ] **Translation plan in place** Languages identified, translators engaged, version control set up.
- [ ] **DoC archived in technical file** Section 8 of the technical documentation index updated with DoC reference.

03

CE marking & putting it together

The sequence from evidence to mark — and the rules that govern it.

CE marking: *the final step*

The CE marking under the CRA is the visible confirmation that a product with digital elements has gone through the required conformity process. It is not a certification mark or a quality grade — it is a legal statement, affixed by the manufacturer, that the conformity assessment is complete, the EU Declaration of Conformity has been signed, and the technical documentation is in order.

Article 30 of the CRA sets out the CE marking obligations. The mark must be affixed to the product and its packaging visibly, legibly, and indelibly. Where this is not possible or appropriate given the nature of the product — for example a software-only product distributed digitally — the mark and the reference number of the DoC must be affixed to the documentation accompanying the product and to the manufacturer's website or distribution platform.

WHAT THE CE MARK SIGNALS

Affixing the CE mark is the manufacturer's declaration that: (1) conformity assessment was completed, (2) the EU Declaration of Conformity was drawn up and signed, and (3) the technical documentation file is complete and accessible. It is a legal attestation, not a warranty. Third parties — including market surveillance authorities, customers, and competitors — can challenge it.

Rules for affixing the CE mark

The CRA applies the standard New Legislative Framework (NLF) rules for CE marking. Key points:

- The mark must use the prescribed graphical format (the CE logo as specified in Regulation (EC) 765/2008). Do not resize the logo below the prescribed minimum height of 5mm.
- No other mark may be affixed that could mislead about the meaning of the CE mark or reduce its legibility.
- If a notified body was involved, its four-digit registration number is affixed immediately after the CE mark.
- The CE mark must appear before the product is placed on the EU market — not after.

The complete sequence

Work through these steps in order. Each step depends on the one before: skipping or reordering them does not accelerate conformity — it invalidates it.

1. **Build and test the product**

   Design, develop, and test the product against the Annex I essential requirements. Document the process in the technical file (Sections 1–3).

2. **Map requirements and apply standards**

   For each Annex I requirement, identify the harmonised standard, common specification, or other solution you are relying on. Record references in Section 4 of the technical file.

3. **Generate the SBOM and establish vulnerability handling**

   Produce the software bill of materials and document your CVD policy and update delivery process (Sections 5 and 6).

4. **State the support period**

   Set and document the support period (Section 7). Make it available to users before placing on market.

5. **Conduct conformity assessment**

   Self-assess (Class I) or engage a notified body (Class II / critical). Record the outcome in Section 9 of the technical file.

6. **Sign the EU Declaration of Conformity**

   Issue the DoC under the Annex V structure (Chapter 02 of this guide). Archive a signed copy in the technical file (Section 8).

7. **Affix the CE mark**

   Mark the product, packaging, and/or accompanying documentation. For Class II / critical, include the notified body number after the CE mark.

FULL CRA APPLICATION: 11 DECEMBER 2027

The CRA's product-placement and technical documentation obligations apply from **11 December 2027**. Vulnerability handling and notification obligations for manufacturers apply from **11 September 2026**. Plan your conformity project backward from December 2027 — for complex Class II products with notified body involvement, preparation time should begin no later than early 2026.

Keeping the CE mark valid

CE marking is not permanent unconditionally. If you make a substantial modification to a product with digital elements already on the market — one that introduces new cybersecurity risks or changes how an existing risk is controlled — the product must go through conformity assessment again before the modified version is placed on the market, and the DoC must be reissued.

Minor bug fixes and security patches that do not change the functionality or risk profile do not trigger a new assessment. Your change management process should include a documented trigger assessment: for each release, record whether the changes constitute a substantial modification under the CRA.

CHAPTER 03 CHECKLIST

- [ ] **Seven-step sequence mapped to a project plan** Owner and target date assigned to each step.
- [ ] **CE mark format confirmed** Correct graphical format sourced; minimum 5mm height respected.
- [ ] **Notified body number included (if applicable)** Four-digit NB number placed immediately after CE mark.
- [ ] **December 2027 deadline in project plan** Backward-scheduled from 11 Dec 2027 with buffer for notified body lead times.
- [ ] **Change management trigger defined** Criteria for what constitutes a substantial modification are documented and owned.

04

Checklist & next steps

Verify your complete technical file, then take the next step.

Master checklist: *your complete technical file*

Use this consolidated checklist once you believe your technical file is complete. Every item should be ticked before you sign the EU Declaration of Conformity. If any item remains open, the file is not ready for conformity assessment or CE marking.

TECHNICAL DOCUMENTATION — NINE ANNEX VII SECTIONS

- [ ] **Section 1 — General description** Product identity, intended purpose, versions, interfaces, data flows, photos/diagrams.
- [ ] **Section 2 — Design, development & production** SDL records, threat models, architecture docs, security testing evidence, build pipeline.
- [ ] **Section 3 — Cybersecurity risk assessment** Versioned risk assessment covering full lifecycle; Annex I mapping embedded or cross-referenced.
- [ ] **Section 4 — Essential requirements** Each Annex I Part I and Part II requirement evidenced or formally marked N/A; standards listed with OJ dates.
- [ ] **Section 5 — SBOM** Machine-readable SBOM (SPDX or CycloneDX); all components including transitive dependencies; update process documented.
- [ ] **Section 6 — Vulnerability handling** CVD policy published; security update delivery tested; ENISA notification process assigned.
- [ ] **Section 7 — Support period** Duration stated, justified, user-facing disclosure in place.
- [ ] **Section 8 — EU Declaration of Conformity** Signed DoC archived; reference recorded in index.
- [ ] **Section 9 — Notified body records** Assessment route confirmed; NB certificate in file (if applicable) or self-assessment record.

DECLARATION & MARKING

- [ ] **EU Declaration of Conformity** Annex V structure complete; all seven elements present; signatory authorised; translations planned.
- [ ] **CE mark affixed** Visible, legible, indelible; correct format; NB number included if Class II/ critical; affixed before market placement.

NEXT STEP

Build your complete technical file

The CRA Facts documentation hub at cra-facts.com/documentation provides article-by-article guidance on each essential requirement, searchable compliance Q&A, and links to the harmonised standards as they are published in the Official Journal.

Subscribe to **The CRA Brief** — our fortnightly digest of CRA regulatory updates, standard adoption news, and enforcement developments — so you never miss a change that could affect your technical file.

cra-facts.com →

QUICK NAVIGATION

Jump to any chapter

Click a tile to go directly to that section.

Explore the documentation hub →

Visit cra-facts.com →

CRA Facts

Your technical file, *assembled withnconfidence.*

cra-facts.com