EUROPEAN COMPLIANCE SUITE
EU AI Act Compliance Evidence Templates

EXPLANATORY NOTICE AND TEMPLATE
Applicability and product classification assessment under the Cyber Resilience Act (Regulation (EU) 2024/2847)

Template reference	ECS-CRA-SCOPE
Version	1.0
Edition	July 2026
Regulation	Regulation (EU) 2024/2847 (Cyber Resilience Act) of 23 October 2024
Instrument addressed	Scope, product classification (Annexes III and IV), economic-operator role and conformity assessment route (Annex VIII)
Intended user	Any manufacturer, importer or distributor making a product with digital elements available on the Union market
Position in the series	Entry document. Complete before the other documents; its findings determine which of them are required and which conformity assessment route applies
Associated templates	ECS-CRA-RECORD — Annex VII technical documentation; ECS-CRA-VULN — vulnerability handling and SBOM; ECS-CRA-REPORT — Article 14 reporting readiness; ECS-CRA-DOC — EU declaration of conformity and CE marking

1. Purpose and context

(1)The Cyber Resilience Act (Regulation (EU) 2024/2847, the “CRA”) entered into force on 10 December 2024. It is the first horizontal Union law to set mandatory cybersecurity requirements for products with digital elements across their whole lifecycle, and it operates as New Legislative Framework product legislation: a product may be made available on the Union market only if it meets the essential requirements in Annex I, and conformity is demonstrated through a conformity assessment, an EU declaration of conformity and the CE marking.

(2)The CRA applies in phases, and the phasing shapes this series. The reporting obligations in Article 14 — notification of actively exploited vulnerabilities and severe incidents — apply from 11 September 2026. The rules on the notification of conformity assessment bodies apply from 11 June 2026. The bulk of the obligations — the essential requirements, conformity assessment, the technical documentation and CE marking — apply from 11 December 2027. A product placed on the market before that date falls under the full requirements only if it is substantially modified after it, but the Article 14 reporting obligations reach products already on the market regardless.

(3)This assessment establishes whether the CRA applies to a given product, in what economic-operator capacity the organisation acts, how the product is classified, and which conformity assessment route consequently applies. It is the entry document of the series and determines which of the other documents the organisation must complete. It does not itself demonstrate conformity; it scopes the work that does.

(4)The classification finding is the pivot of the whole exercise. Most products with digital elements are unclassified “default” products and may use the internal-control conformity route without a notified body. Products named in Annex III are “important” (Class I or Class II) and face a stricter route; products named in Annex IV are “critical” and may be required to hold a European cybersecurity certificate. Because the route, the cost and the timeline all follow from classification, a defensible classification finding recorded here is the foundation on which the rest of the file is built.

RELEVANT LEGAL TEXT

Article 3 CRA — Definitions (extracts).

A "product with digital elements" means a software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately. A "manufacturer" means a natural or legal person who develops or manufactures products with digital elements, or has them designed, developed or manufactured, and markets them under its name or trademark. "Making available on the market" means the supply of a product for distribution or use on the Union market in the course of a commercial activity, whether in return for payment or free of charge.

Article 6 and Annexes III and IV — Classification.

Products listed in Annex III are important products with digital elements (Class I or Class II). Products listed in Annex IV are critical products with digital elements. Where a product falls within more than one category, the category entailing the stricter conformity assessment obligation applies. Classification follows the product's core functionality.

Article 32 and Annex VIII — Conformity assessment.

The manufacturer shall demonstrate conformity with the essential requirements by one of the applicable procedures: internal control (Module A); EU-type examination (Module B) followed by conformity to type (Module C); or full quality assurance (Module H). Default products may use internal control. Important products face a route constrained by the availability of harmonised standards; critical products may require a European cybersecurity certificate.

Article 14 CRA — Reporting (application date).

Manufacturers shall notify actively exploited vulnerabilities and severe incidents affecting the security of their products with digital elements through the single reporting platform. This obligation applies from 11 September 2026, ahead of the full application of the Regulation on 11 December 2027, and reaches products already made available on the Union market.

2. How to use this assessment

(5)The assessment proceeds through six findings, completed in order. Each can close or narrow the exercise, and each calls for reasoning rather than a bare answer.

- Finding A — Is the product a "product with digital elements" within scope, and does an exclusion apply?
- Finding B — In what economic-operator capacity does the organisation act — manufacturer, importer or distributor?
- Finding C — Is the product default, important (Annex III, Class I or II) or critical (Annex IV)?
- Finding D — Which conformity assessment route follows from the classification?
- Finding E — What is the support period, and how was it determined?
- Finding F — Which documents in the series, and which obligations by which date, consequently apply?

3. The six findings

3.1. Finding A — scope and exclusions

(6)A product with digital elements is a software or hardware product, and its remote data processing solutions, whose intended or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network. The definition is broad: it captures final products and components placed on the market separately, hardware and software alike. The starting presumption for a connected product is that it is in scope.

(7)Several exclusions and interactions must be checked rather than assumed. Products already covered by equivalent Union cybersecurity requirements — certain medical devices, motor vehicles, civil aviation and marine equipment products — are carved out or handled under their sectoral regimes. Software provided as a service (SaaS) is generally outside the CRA except where it constitutes a remote data processing solution integral to a product. Free and open-source software developed or supplied outside the course of a commercial activity is outside scope, and a lighter regime applies to "open-source software stewards." Each exclusion relied on should be recorded with its basis, because an exclusion asserted but not made out leaves the organisation without a file it was required to hold.

3.2. Finding B — economic-operator capacity

(8)The CRA assigns obligations by role. The manufacturer carries the substantive obligations — the essential requirements, the technical documentation, conformity assessment, the declaration of conformity, CE marking and Article 14 reporting. Importers must verify that the manufacturer has carried out conformity assessment, drawn up the technical documentation and affixed the CE marking, and must not place a non-conforming product on the market. Distributors must act with due care in relation to the requirements. An organisation that markets a product under its own name or trademark, or that substantially modifies a product already on the market, is treated as a manufacturer and takes on the manufacturer's obligations — a trap for own-branding and integration businesses that must be settled here.

3.3. Finding C — classification

(9)Classification determines the conformity assessment route and follows the product's core functionality. A default product is one named in neither Annex III nor Annex IV; the large majority of products with digital elements are default. A product named in Annex III is important — Class I or, for the more sensitive categories, Class II. A product named in Annex IV is critical. Where a product could fall in more than one category, the category entailing the stricter obligation applies.

(10)Annex III Class I includes, among others, identity and privileged-access management, standalone and embedded browsers, password managers, antivirus, VPNs, network management systems, SIEM systems, boot managers, PKI and certificate-issuance software, physical and virtual network interfaces, operating systems, routers, modems and switches, certain microprocessors, microcontrollers, ASICs and FPGAs with security functionality, smart-home assistants and security products, internet-connected toys and certain wearables. Class II is narrower and more sensitive — hypervisors and container runtimes, firewalls and intrusion detection or prevention systems, and tamper-resistant microprocessors and microcontrollers. The implementing regulation on product categories provides the official technical descriptions and should be consulted for borderline products; the classification recorded here should cite the specific Annex III or IV entry relied on, or record the reasoned conclusion that none applies.

3.4. Finding D — conformity assessment route

(11)A default product may use internal control (Module A): the manufacturer draws up the technical documentation, ensures the design, development, production and vulnerability-handling processes deliver conformity, and affixes the CE marking on its own responsibility, without a notified body. An important product may use internal control only where harmonised standards (or a common specification, or a relevant cybersecurity certification scheme) covering the applicable requirements exist and are applied in full; otherwise it must use EU-type examination (Module B) plus conformity to type (Module C), or full quality assurance (Module H), each involving a notified body. A critical product may additionally be required to hold a European cybersecurity certificate under a designated scheme. Because the availability of harmonised standards governs whether an important product needs a notified body, and the first CRA harmonised standards are expected only over the course of 2026–2027, the route recorded here should note the standards position as at the date of assessment.

3.5. Finding E — support period

(12)The manufacturer must determine a support period during which vulnerabilities are handled and security updates provided, reflecting how long the product is reasonably expected to be in use; the CRA anchors an expectation of at least five years for many products unless the nature of the product justifies otherwise. The support period drives the ten-year documentation retention (which runs from placing on the market or the end of the support period, whichever is longer), the duration of the vulnerability-handling obligations, and the information given to users under Annex II. The reasoning that fixed the support period is recorded here and carried into the technical file.

3.6. Finding F — documents and dates

(13)The assessment closes by determining what the organisation must produce and by when. For a manufacturer, that is the Annex VII technical documentation (ECS-CRA-RECORD) with its Annex I Part I compliance matrix; the vulnerability-handling and SBOM evidence (ECS-CRA-VULN) implementing Annex I Part II; the Article 14 reporting readiness (ECS-CRA-REPORT), which is the first obligation to bite, from 11 September 2026; and the EU declaration of conformity, CE marking record and Annex II user information (ECS-CRA-DOC). The dated sequence matters: reporting readiness is needed in 2026, the full conformity file by 11 December 2027.

4. Penalties and enforcement

(14)Enforcement is by national market surveillance authorities, which may require corrective action, restrict or prohibit a product, or order withdrawal or recall. The penalty ceilings are among the highest in Union product law: up to €15 million or 2.5% of total worldwide annual turnover, whichever is higher, for breaches of the essential requirements or the manufacturer obligations. The severity of the ceiling and the ten-year retention of the technical file together make a documented, defensible conformity position — rather than an undocumented assumption of compliance — the prudent posture from the outset.

5. Review

(15)This assessment is renewed when the product is substantially modified, when a change in the product or its functionality affects its classification, when the organisation’s role changes, when harmonised standards affecting the conformity route are published, and in any event at intervals not exceeding twelve months while the product remains on the market.

Annex

Template for the applicability and product classification assessment under the Cyber Resilience Act (Regulation (EU) 2024/2847)

Assessment version	*Version identifier, with references to earlier versions where applicable.*
Last updated	*DD.MM.YYYY*
Prepared by	*Name, function and role of the person responsible for the accuracy of this assessment.*
Product identification	*Name, type and version(s) of the product with digital elements assessed.*
Classification	*Internal / shareable with a notified body / shareable with authorities.*

1. Product and organisation

Product with digital elements	*Name, type and any additional information enabling unique identification. For a component placed on the market separately, identify it as such.*
Connectivity	*The direct or indirect logical or physical data connection to a device or network, in intended use or reasonably foreseeable use.*
Organisation	*Legal name, seat and legal form.*
Date of assessment	*DD.MM.YYYY*
Legal text verified on	*Date the applicable provisions were checked against the in-force text of the CRA and its implementing and delegated acts.*

2. Finding A — scope and exclusions

Product with digital elements?	*Confirm the product and, where applicable, its remote data processing solution fall within the definition.*
Sectoral carve-outs	*Whether the product is covered by an equivalent sectoral regime (e.g. medical devices, motor vehicles, civil aviation, marine equipment) and its CRA treatment.*
SaaS / open-source position	*Whether any part is SaaS outside scope, or free and open-source software outside the course of a commercial activity, or whether the open-source-steward regime applies.*
Conclusion	*The CRA applies / does not apply to this product, with the basis for any exclusion relied on.*

3. Finding B — economic-operator capacity

Capacity	*Manufacturer / importer / distributor.*
Own-branding or substantial modification	*Whether the organisation markets under its own name or trademark, or substantially modifies a product on the market — either of which makes it a manufacturer.*
Authorised representative	*Where the manufacturer is established outside the Union, the authorised representative appointed, if any.*

4. Finding C — classification

Classification follows core functionality. Where more than one category fits, the stricter applies. Cite the specific Annex entry relied on, or record the reasoned conclusion that none applies.

Tier	Applies?	Annex entry / basis
Default (named in neither Annex III nor IV)		
Important — Annex III Class I		
Important — Annex III Class II		
Critical — Annex IV		

Classification conclusion	*The product is default / important Class I / important Class II / critical, with the core-functionality reasoning.*

5. Finding D — conformity assessment route

Harmonised standards position	*Whether harmonised standards, a common specification or a relevant certification scheme covering the applicable requirements exist and can be applied in full, as at the date of assessment.*
Route	*Internal control (Module A) / EU-type examination + conformity to type (Modules B+C) / full quality assurance (Module H). For important products, justify why internal control is or is not available.*
European cybersecurity certificate	*For critical products, whether a certificate under a designated scheme is required.*
Notified body	*Where a notified body is required, its identity once engaged.*

6. Finding E — support period

Support period	*The determined support period and the date it ends.*
Basis	*The reasoning — expected use, product nature, comparable products — that fixed the period.*
Retention consequence	*The resulting documentation retention date: placing on the market or end of support period, whichever is longer, plus ten years.*

7. Finding F — documents and dates

Documents required	*Which of ECS-CRA-RECORD, ECS-CRA-VULN, ECS-CRA-REPORT and ECS-CRA-DOC are required.*
Article 14 reporting readiness (from 11.09.2026)	*Owner and target date for reporting readiness — the first obligation to apply.*

Full conformity file (from 11.12.2027)	*Owner and target date for the technical documentation, conformity assessment, declaration of conformity and CE marking.*
Responsible owners	*Who is responsible for each consequent step and by when.*

8. Review

Next scheduled review	*DD.MM.YYYY, no later than twelve months after the date of assessment.*
Trigger events recorded	*The changes — substantial modification, reclassification, role change, publication of harmonised standards — that would require reassessment before then.*

9. Version history and declaration

Version	Date	Nature of change or review	Approved by

Declaration

The findings above are made in good faith and, to the knowledge of the signatory, are accurate and complete as at the date of signature. Where a finding could not be made on the information available, the gap and the reason for it have been recorded in the relevant field.

Name	
Function	
Date	
Signature	