

Compliance Engineering under the EU Cyber Resilience Act: Timelines, Obligations, and SBOM-Driven Product Security

Abdelkarim Erradi

ORCID: 0000-0002-8333-3454

Department of Computer Science and Engineering, Qatar University, Doha, Qatar

Leonardo Badia

ORCID: 0000-0001-5770-1199

Department of Information Engineering, University of Padova, Padova, Italy

Correspondence: Abdelkarim Erradi · contact details held in the journal record

Publication history. Assigned by the publisher to Cybersecurity Advances, Volume 2, Issue 1 (2025). This publisher-authorized digital edition was released on 29 October 2026 from the supplied final 2025 manuscript. Review-stage notices were removed and journal typography, pagination, metadata, and accessibility were normalized; substantive scholarly content was preserved.

© 2025 the author(s). Published by AlphaTech Scholarly Press under the Creative Commons Attribution 4.0 International License (CC BY 4.0). No DOI is displayed unless and until registration is independently verified.

Background: The EU Cyber Resilience Act (CRA, Regulation (EU) 2024/2847) entered into force on 10 December 2024, and 2025 was its preparation year: the Commission's delegated acts took shape, harmonized-standardization work began, and manufacturers confronted the obligations timetable — vulnerability and incident reporting from 11 September 2026 (24-hour early warning, 72-hour notification), full application including CE-marking consequences on 11 December 2027, and open-source steward duties from the same date.

Objective: We translate the CRA's legal obligations into an engineering program: what a manufacturer of products with digital elements must build, in what order, to be compliant by construction rather than by remediation. **Methods:** Documentary analysis of the CRA's obligations and official Commission guidance; mapping of obligations to security-engineering practices (SSDF, SBOM, SLSA-class process evidence); and construction of an SBOM-driven vulnerability-management pipeline aligned with the Act's reporting duties.

Results: The CRA converts product security from a best practice into a lifecycle *obligation*: secure-by-default configuration, risk assessment, security-update handling across a support period of at least five years, and 24/72-hour reporting of actively exploited vulnerabilities and severe incidents. The SBOM is the load-bearing artifact — it is what makes feed correlation, triage, and notification computable at product scale. The engineering-critical path runs through 2026: reporting obligations arrive a full fifteen months before full application, so the reporting pipeline must exist before the conformity machinery does. **Conclusions:** Organizations should treat 2025–2026 as the compliance-engineering window: build the SBOM pipeline, stand up the reporting process, and align development practice with the harmonized standards — because the CRA makes security a property of the market, enforced through product-safety law.

Keywords: Cyber Resilience Act; product security; SBOM; vulnerability management; secure by default; CE marking; security engineering; EU regulation

Contribution statement. This paper makes four contributions: (1) a verified obligations timeline for the CRA with the engineering-critical path identified (reporting before conformity); (2) a mapping of CRA duties to security-engineering practices and artifacts; (3) an SBOM-driven vulnerability-management pipeline aligned with the Act's 24/72-hour reporting duties; and (4) a preparation roadmap for manufacturers of products with digital elements, sized by company class.

1. Introduction

For three decades, software product security in the EU market was governed by incentive, not law: vendors shipped what they shipped, and the market's sanction for insecurity was reputational. The **Cyber Resilience Act** changes the legal category. Regulation (EU) 2024/2847 entered into force on 10 December 2024 and makes cybersecurity an essential-requirements matter for *products with digital elements* — hardware and software placed on the EU market — with conformity assessment, CE marking, and market-surveillance consequences for non-compliance [1]. The Act's timetable is staggered: manufacturers' **reporting obligations** — actively exploited vulnerabilities and severe incidents, with a 24-hour early warning and 72-hour full notification to ENISA and the

CSIRTs network — begin on **11 September 2026**; the full regime, including the security requirements that gate CE marking, applies from **11 December 2027**; and open-source software stewards assume their specific notification duties from the same December 2027 date [1][2][3].

2025 was, in consequence, the Act's preparation year — the interval in which the delegated and implementing acts were settled (including a reporting delegated act adopted on 11 December 2025), harmonized-standardization work advanced, and manufacturers made their build-or-buy decisions about compliance infrastructure [2]. This paper addresses the audience for whom the Act is an engineering program rather than a legal text: the teams that must make products with digital elements *compliant by construction*.

The paper's central engineering claim is that one artifact carries the Act's operational weight: the **software bill of materials (SBOM)**. The CRA's vulnerability-handling and reporting duties are computable only if a manufacturer can, for any released product version, enumerate the product's software composition, correlate it against vulnerability and exploit intelligence, determine contextual severity, and produce the notifications the timetable demands. That chain is exactly the SBOM-driven pipeline the supply-chain security literature has advocated for a decade [4][5][7]; the CRA makes it mandatory, on a clock.

1.1 Research questions

RQ1: What obligations does the CRA impose, on what dates, on which economic operators? **RQ2:** How do those obligations map onto security-engineering practices and artifacts? **RQ3:** What does an SBOM-driven vulnerability-management pipeline that satisfies the Act's reporting duties look like? **RQ4:** What preparation roadmap should manufacturers follow through 2026-2027?

1.2 Contributions

(1) The verified obligations timeline with the engineering-critical path identified (Section 3, Figure 1, Table 1) (RQ1). (2) The obligations-to-practice mapping (Section 4, Figure 2, Table 2) (RQ2). (3) The reporting-aligned SBOM pipeline (Section 5, Figure 3, Table 3) (RQ3). (4) A class-sized preparation roadmap (Section 6) (RQ4).

2. Background

2.1 The CRA in the regulatory stack

The CRA completes an EU product-security architecture that the 2024 instruments began: NIS2 (Directive (EU) 2022/2555) governs *operators* of essential and important entities; the CRA governs *products* with digital elements placed on the market, irrespective of the operator's sector [1][8]. The two regimes interlock — a manufacturer is often also a NIS2 entity — but their compliance logics differ: NIS2 is risk-management and accountability law; the CRA is essential-requirements and market-surveillance law. The CRA also operationalizes, in binding form, the supply-chain transparency agenda that U.S. policy began with EO 14028 and the NTIA SBOM minimum elements [4][5], and it aligns with the secure-development framing of NIST's SSDF [6].

2.2 The CRA's security-engineering core

The Act's Annex I essential requirements read as a security-engineering curriculum: secure-by-default configurations; protection against unauthorized access; secure development practice (including vulnerability handling and source-code documentation duties); risk assessment appropriate to the product's risk class; and — the operational core — the manufacturer's responsibility to handle vulnerabilities and provide security updates throughout a support period of at least five years (or the product's expected lifetime, where longer) [1]. The reporting article (Art. 14, with Art. 71's phased application) then attaches the clock: 24-hour early warning of actively exploited vulnerabilities or severe incidents, 72-hour notification, and final reports tied to corrective-action availability [2][3]. For engineering teams, the Act is best read as *lifecycle security with evidence duties*: every claim about the product's security must be documentable, and every incident must move on a timetable.

3. The Obligations Timeline and the Critical Path (RQ1)

Figure 1 presents the timetable; Table 1 details it. The engineering-critical path runs through 2026: reporting obligations begin on 11 September 2026 — fifteen months before full application — which means the notification pipeline (detection, triage, notification drafting, ENISA/CSIRT submission) must be operational well before the conformity machinery is finished [2][3]. A manufacturer that begins building its reporting process in 2027 will be non-compliant

for over a year. The December 2025 delegated act on reporting operationalized the notification formats and mechanics, completing the specification the pipeline must implement [2].

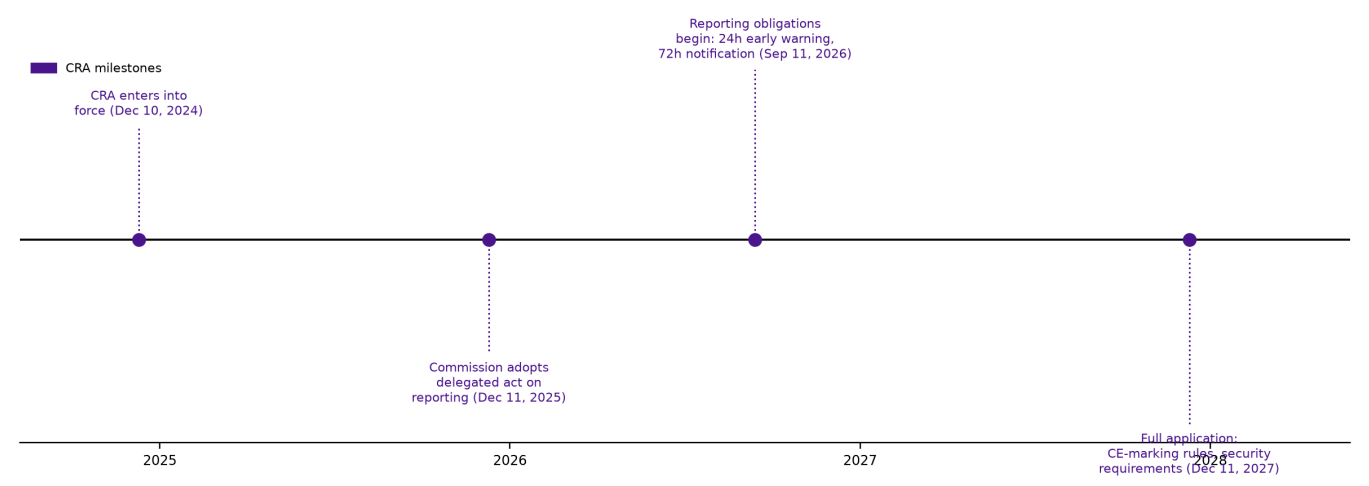


Figure 1. The CRA timetable: entry into force (Dec 2024), the reporting delegated act (Dec 2025), reporting obligations (Sep 2026), and full application (Dec 2027) [1][2][3].

Milestone	Date	What applies	Source
CRA entry into force	Dec 10, 2024	The Regulation becomes binding law; transition clock starts	[1][3]
Reporting delegated act	Dec 11, 2025	Commission act operationalizing notification formats and mechanics	[2]
Reporting obligations begin	Sep 11, 2026	Manufacturers report actively exploited vulnerabilities & severe incidents: 24h early warning, 72h notification, final reports on the corrective-action clock	[2][3]
Full application	Dec 11, 2027	Essential requirements, CE-marking consequences, market surveillance; open-source steward notification duties (Art. 24(3))	[1][2][3]
Support-period duty	Ongoing from Dec 2027	Security updates for at least 5 years (or expected lifetime, if longer)	[1]

Table 1. CRA obligations and key dates [1][2][3].

4. Obligations as Engineering Practice (RQ2)

Figure 2 maps the Act's duties onto the product lifecycle; Table 2 details the operator-class duties. The mapping's purpose is to convert legal text into backlog. Three mappings deserve emphasis.

Secure by default is a product requirement, not a preference. The essential requirements demand that products be secure by default in configuration — the practice the CISA Secure-by-Design initiative had urged [10] — now with market-surveillance consequences. For engineering teams this means default-hardening work (password-free onboarding, minimal open services, safe update mechanisms) enters the *release checklist*, not the roadmap.

The support period is an SLO. At least five years of security updates — or the expected lifetime where longer — makes update engineering (build, test, distribute, and *drive adoption* of updates) a formal obligation with a duration. Update-mechanism engineering — signed, automatic, verifiable update channels, the artifact-signing class that sigstore provides [11] — becomes compliance-critical infrastructure [6][7][11].

Process evidence is product evidence. The Act's conformity assessment reviews technical documentation; an SBOM, a vulnerability-handling process record, and secure-development process evidence (SSDF-aligned [6], SLSA-class provenance [7]) are the artifacts by which the product's security claims are examined [5][8]. Security engineering under the CRA is, observably, documentation engineering — the practices must exist *and be provable*. (The Act grades products by risk class; Annex III defines the high-risk class — products combining digital elements with critical infrastructure or safety functions — which faces stricter conformity assessment [1].)

The CRA turns product security into a lifecycle obligation

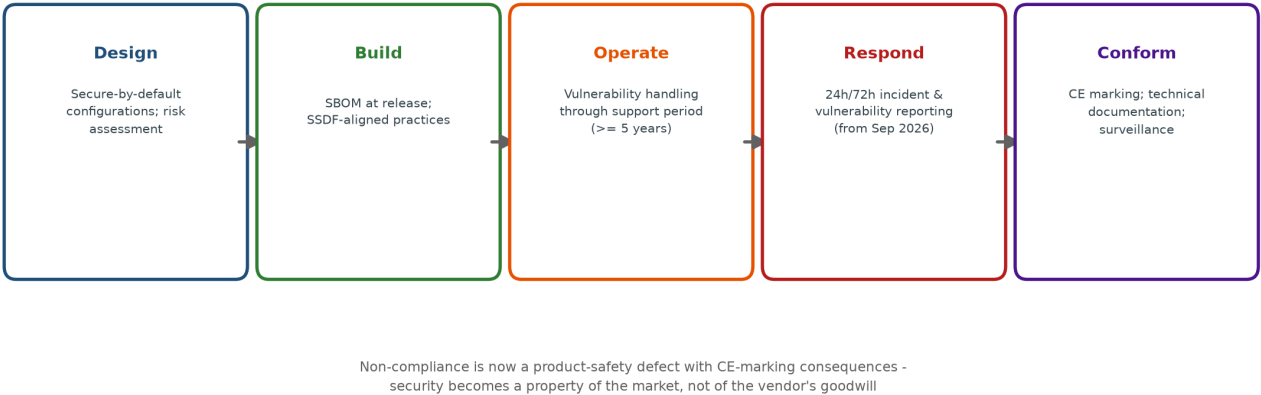


Figure 2. Product-security lifecycle obligations under the CRA [1].

Operator class	Core CRA security duties (engineering-relevant)
Manufacturers	Secure-by-default configuration; vulnerability handling & disclosure; security updates through the support period; conformity & technical documentation; CE marking; 24h/72h incident & vulnerability reporting (from Sep 2026)
Importers	Verify CE marking and documentation; ensure traceability; act on non-compliant products
Distributors	Verify conformity markers and support-period information; handle vulnerabilities per role
Open-source stewards	Duties attach from Dec 2027 (Art. 24(3)): security documentation and notification duties for stewarded software made available in the EU

Table 2. CRA economic-operator duties relevant to security engineering [1].

5. The SBOM-Driven Reporting Pipeline (RQ3)

Figure 3 presents the five-stage pipeline that the reporting duties demand. Stage 1: author the SBOM at release — component inventory with identifiers (PURL/CPE), dependency depth, and provenance metadata, with reproducible-build practices making that provenance verifiable rather than asserted [5][9]. Stage 2: continuous correlation of the SBOM against vulnerability feeds and exploit intelligence, with VEX-style exploitability claims to suppress false urgency [7]. Stage 3: contextual triage — severity in product context, not component-generic scoring. Stage 4: patch, mitigate, and drive update adoption through the product's update channel. Stage 5: notification — the 24-hour early warning and 72-hour full notification of actively exploited vulnerabilities or severe incidents, with final reports on the corrective-action clock [2][3].

The pipeline's non-obvious engineering requirements are three. **Speed:** the 24-hour clock begins at awareness, which means detection-to-decision latency must be engineered, not assumed. **Attribution accuracy:** notifications that misidentify affected products create legal exposure both ways; the SBOM must be version-precise. **Steward duties for open source:** stewards of open-source software made available in the EU assume notification duties from December 2027 — a novel obligation on foundations and maintainers that the ecosystem's tooling does not yet routinely satisfy [2][3].

SBOM-driven vulnerability management under the CRA



The SBOM is the instrument that makes steps 2-5 computable at product scale

Figure 3. SBOM-driven vulnerability management aligned with the CRA's reporting duties [2][5][6].

Pipeline stage	Mechanism	CRA obligation served
1. Author SBOM at release	Component inventory with identifiers, dependency depth, provenance	Technical documentation; vulnerability-handling duty (Art. 14)
2. Correlate feeds + VEX	Continuous matching of SBOM against vulnerability & exploit intelligence; exploitability claims	Awareness triggering the 24h early-warning clock
3. Contextual triage	Severity assessed in product context, not component-generic scoring	Severe-incident determination (Art. 14)
4. Patch / mitigate & drive adoption	Signed update channel; customer update engineering	Security-update support period (>= 5 years)
5. Notify ENISA / CSIRTs	24h early warning; 72h full notification; final report after corrective measure	Art. 14 reporting (from Sep 11, 2026)

Table 3. SBOM-driven vulnerability management mapped to CRA reporting obligations [1][2][5][6].

6. The Preparation Roadmap (RQ4)

For **large manufacturers**, 2025-2026 is an integration year: SBOM pipelines into CI/CD, reporting tooling into incident response, conformity documentation into release management, and harmonized-standard alignment into design reviews. For **SMEs**, the Act's proportionality provisions help but the engineering demand does not shrink proportionally; the pragmatic path is (1) SBOM generation from the build system (largely automatable), (2) a vulnerability-triage process sized to the product's risk class, and (3) a rehearsed notification procedure — the three artifacts on which the 2026 clock will bite first. For **open-source stewards**, 2026 is the year to establish the steward role, the notification contact, and the cooperation channels with commercial downstreams [2][3]. Across all classes, the sequencing rule is the critical path's: *reporting first, conformity second* — the September 2026 clock does not wait for December 2027.

7. Limitations and Threats to Validity

Construct validity. The obligations-to-practice mapping is an engineering interpretation of legal text; specific deployments require counsel review, particularly around product risk classification. **Internal validity.** The delegated-act landscape was evolving through 2025 (including the December 2025 reporting act); later acts refine the pipeline's mechanics. **External validity.** The roadmap is calibrated for products with digital elements under the Act's default conformity path; Annex III high-risk-class products face additional conformity requirements not analyzed here. **Temporal scope.** Frozen at year-end 2025; harmonized standards, guidance, and market-surveillance practice will continue to develop into the application period.

8. Conclusion

The Cyber Resilience Act ends the era in which product security was a virtue. It is now a condition of the market, with a timetable: report from September 2026, comply fully by December 2027, keep the product secure for at least five years. The engineering translation is direct — secure defaults in the release checklist, update infrastructure as compliance-critical, process evidence as product evidence, and an SBOM pipeline that can correlate, triage, and notify on a 24/72-hour clock. The critical path runs through 2026; the organizations that build their reporting pipelines first will meet the Act's deadlines as a by-product of engineering they should have been doing anyway. The CRA's deepest effect may be exactly that: it converts the market's security externality into an engineering requirement, and the products that ship after 2027 will carry its discipline inside them.

Declarations

Funding. This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

CRedit contribution statement. Abdelkarim Erradi: conceptualization, regulatory analysis, writing – original draft. Leonardo Badia: validation, product-scope analysis, writing – review & editing. (Corresponding author: Abdelkarim Erradi.)

Competing interests. The authors declare no competing interests.

Data and code availability. No new datasets were generated; all regulatory claims trace to the cited official sources [1][2][3].

Ethics and dual-use. Not applicable; the paper contains no offensive content.

AI assistance declaration. AI-based tools were used in a limited supporting capacity (literature search, figure preparation, and language editing); all research content, analysis, and conclusions were produced, reviewed, and verified by the authors, who take full responsibility for the work.

References

- [1] Regulation (EU) 2024/2847 of the European Parliament and of the Council laying down measures for a high common level of cybersecurity across the Union (Cyber Resilience Act), adopted 23 October 2024, published in the Official Journal of the European Union, 20 November 2024 (in force 10 December 2024).
- [2] European Commission, "Cyber Resilience Act - Reporting obligations" (incl. delegated act adopted 11 December 2025), Shaping Europe's Digital Future. [Online]. Available: <https://digital-strategy.ec.europa.eu/en/policies/cra-reporting>
- [3] National Cyber Security Centre (Ireland), "Cyber Resilience Act - key enforcement dates," 2025. [Online]. Available: <https://www.ncsc.gov.ie/cra>
- [4] Executive Order 14028, "Improving the Nation's Cybersecurity," 86 FR 26633, May 12, 2021.
- [5] National Telecommunications and Information Administration, "The Minimum Elements for a Software Bill of Materials (SBOM)," Jul. 2021. [Online]. Available: <https://www.ntia.gov/report/2021/minimum-elements-software-bill-materials-sbom>
- [6] NIST, "Secure Software Development Framework (SSDF) v1.1," NIST SP 800-218, Feb. 2022. doi: 10.6028/NIST.SP.800-218.
- [7] Open Source Security Foundation (OpenSSF), "SLSA Specification v1.0," 2023. [Online]. Available: <https://slsa.dev/spec/v1.0/>
- [8] Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2), OJ L 333, Dec. 2022.
- [9] C. Lamb and S. Zacchiroli, "Reproducible builds: increasing the integrity of software supply chains," IEEE Software, vol. 39, no. 2, pp. 62-70, Mar./Apr. 2022. doi: 10.1109/MS.2020.2996796.
- [10] Cybersecurity and Infrastructure Security Agency, "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default," Apr. 2023.
- [11] Open Source Security Foundation (OpenSSF), "sigstore: software signing transparency," 2025. [Online]. Available: <https://www.sigstore.dev>