

Secure by design — by law.

The proof lives in your SDLC.

The Cyber Resilience Act makes manufacturers of every product with digital elements prove secure development: risk assessments, SBOMs, access control, activity logging, vulnerability handling, 24-hour reporting and ten-year documentation. That proof is created — or lost — in the software development lifecycle, where developers, contractors, non-human identities and AI coding agents build the products the CRA regulates.

LIVE NOW

In force & preparing

CRA in force since 10 Dec 2024; notified-body chapter applies since 11 Jun 2026

11 SEP 2026

Reporting begins

Art. 14 — weeks away: 24 h early warning, 72 h notification via ENISA's Single Reporting Platform

11 DEC 2027

Full application

Essential requirements, conformity assessment, technical documentation and CE marking

≥5 YEARS

Support period

Vulnerability handling through the declared support period; security updates available for ten years

Regulation (EU) 2024/2847 — published 20 Nov 2024, in force 10 Dec 2024. Timeline per the European Commission's CRA implementation pages; the ENISA Single Reporting Platform is in testing and operational by 11 Sep 2026.

EXECUTIVE SUMMARY

The CRA regulates how software is made — not just what ships

The obligations that decide conformity are **development-process obligations**: a documented risk assessment driving design (Art. 13), essential requirements including protection against unauthorized access and logging of relevant internal activity (Annex I Part I), an SBOM with component due diligence (Annex I Part II, Art. 13(5)), vulnerability handling across a declared support period (Art. 13(8–9)), exploited-vulnerability and incident reporting on 24 h / 72 h clocks (Art. 14), and an Annex VII technical-documentation package retained for ten years (Art. 31).

Scanners, SBOM generators and patching pipelines cover the **artifact layer**. What remains chronically missing is the **development-evidence layer**: who — human, bot or AI agent — wrote, approved and shipped each component, whether access to code and build systems was actually controlled, and whether the logs the CRA demands exist for every release. BlueFlag Security is the system of record for precisely that: software identity, change provenance and SDLC governance evidence.

THE BLIND SPOT

THE TYPICAL CRA STACK — WATCHES THE ARTIFACT

- SAST / SCA scanning · SBOM generators
- Patching pipelines · runtime & EDR · GRC

Necessary for Annex I and vulnerability handling — but none of it proves who built the product, who had access, or that secure development actually happened.



THE BLUEFLAG QUESTION — CAN YOU PROVE SECURE DEVELOPMENT?

- › Who — human, bot or AI agent — wrote and approved this component?
- › Was access to code and build systems controlled?
- › Do the Annex I activity logs exist — for every release?
- › Can you trace an exploited CVE to commit and owner in minutes?

WHY NOW

Four reasons the SDLC decides CRA compliance



DEADLINE

Reporting in weeks

Art. 14 goes live 11 Sep 2026:
24 h early warning, 72 h full notification, final report within 14 days (vulnerabilities) or one month (incidents).



SCOPE

Every digital product

Hardware and software with any direct or indirect data connection — CE marking now certifies CRA conformity for market access.



EVIDENCE

A documentation regime

Risk assessment, SBOM, activity logs and the Annex VII package — retained for ten years, produced to authorities on request.



PENALTIES

Real teeth

Fines up to €15M or 2.5% of global turnover for breaching essential requirements or the Article 13–14 obligations.

THE FRAMEWORK

One platform, three roles in your CRA program

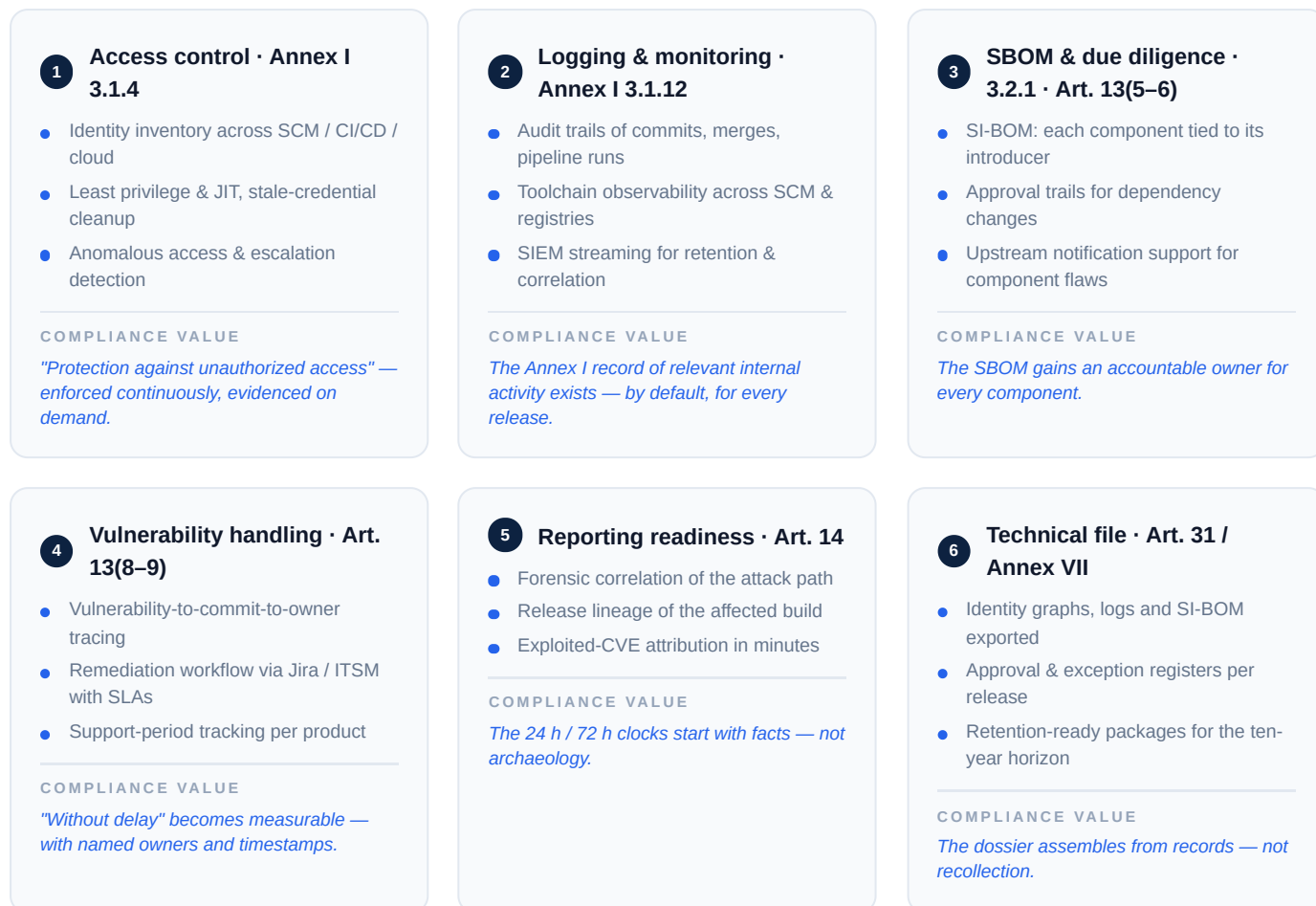
ROLE	CUSTOMER CHALLENGE	BLUEFLAG SECURITY VALUE
1 · Prove secure development	Annex I demands access control and logging of relevant internal activity; conformity assumes secure processes — not just scanned artifacts.	The Activity Intelligence Graph attributes every commit, review, build and deployment to a human, NHI or AI agent; least privilege is continuously enforced across SCM, CI/CD and registries — Annex I 3.1.4 access control and 3.1.12 logging made operational and exportable.
2 · Own the supply chain	The SBOM lists components; due diligence (Art. 13(5)) demands knowing and governing how each one entered the product.	The SI-BOM (Software Identity BOM) ties every dependency to the identity that introduced it, with approval trails for component changes and upstream-notification support when a component's flaw is found (Art. 13(6)) — pairing with CycloneDX/SPDX generators for full depth.
3 · Respond & report on the clock	The 24 h / 72 h clocks start at awareness; manual reconstruction across Git, CI and ticketing blows the window.	Vulnerability-to-commit-to-owner trace in minutes: forensic lineage of the affected release, the introducing change and the accountable identity — feeding the Single Reporting Platform notifications and the final report with facts (Art. 14).

Positioning discipline: BlueFlag does not scan for CVEs, deploy patches or file the ENISA reports, and it does not make conformity determinations. It makes the development-process controls the CRA samples operational — and keeps the evidence.

ARTICLE-BY-ARTICLE

Where BlueFlag carries the obligation

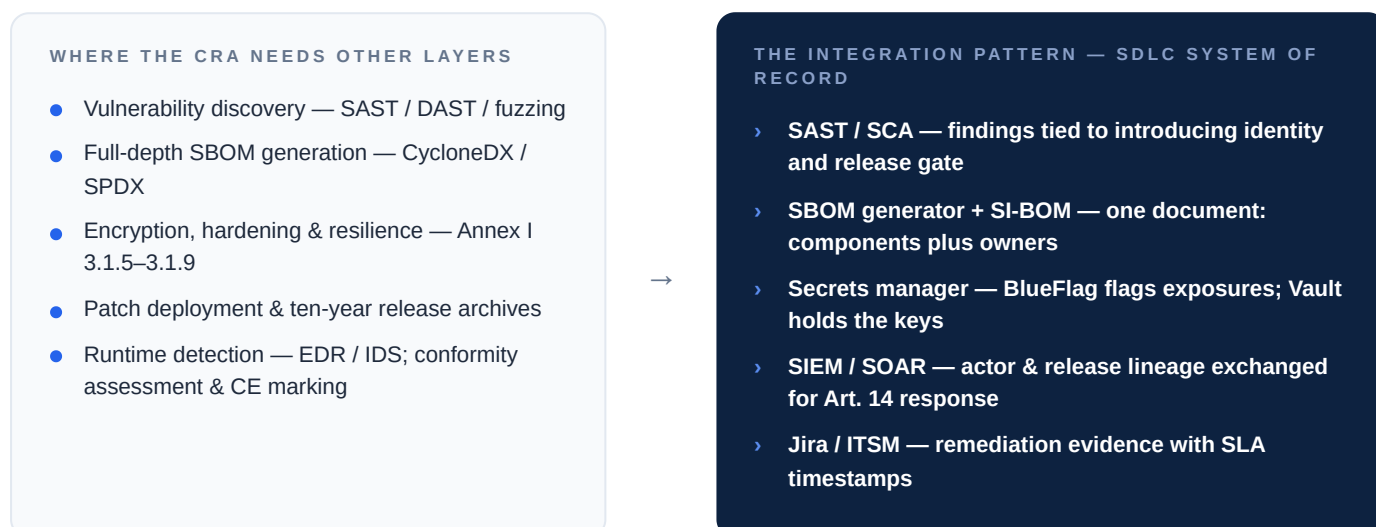
Six obligations where the CRA requires exactly what an identity-first SDLC control plane produces — mapped from the full control-mapping analysis.



COMPLETE PROVENANCE ACROSS THE PRODUCT LIFECYCLE



HONEST SCOPE · NOT SUFFICIENT ALONE



THE OPERATING MODEL

Report-ready in weeks. Conformity-ready by December 2027.



Weeks 0–8 — Report-ready by 11 Sep

Identity and toolchain discovery; forensic lineage live; intake–triage–escalation workflow wired to your Single Reporting Platform process.



Q4 2026 — Govern the estate

Organization-wide rollout, least privilege and stale-account cleanup across SCM / CI/CD, policy definition and developer onboarding.



H1 2027 — Supply chain & vulns

SI-BOM plus SBOM tooling, SAST/SCA integration, vulnerability-triage workflow with SLAs, support periods declared per product.



H2 2027 — Conformity by 11 Dec

Internal audit, Annex VII package assembled from BlueFlag outputs, notified-body engagement where required, CE marking.

WHY EACH STAKEHOLDER SHOULD CARE

CISO / Product Security	Annex I made operational: access control, least privilege, activity logging and anomaly detection across the pipelines that build every CE-marked product — with the Art. 14 forensic trail ready before 11 September.
GRC / Compliance	The Annex VII technical file assembles from live records — risk-assessment inputs, SI-BOM, logs, approvals — retained across the ten-year horizon and produced to market-surveillance authorities on request.
Product / R&D Leadership	Support periods, component ownership and update evidence tracked per product line — the data valuation, roadmap and end-of-support decisions rest on.
Legal / Regulatory	Clean role separation: BlueFlag supplies the attributable technical record; counsel owns product classification (Annexes III/IV), the conformity route and the EU Declaration of Conformity.
Engineering / Platform	Controls live in the existing path to merge — no parallel compliance workflow; AI agents and automation keep shipping, with a named owner behind every component and change.

EXECUTIVE MESSAGE

“The CRA makes secure development a market-access requirement. BlueFlag is the system of record that proves it — who built the product, who had access, and that the controls held — release by release, across the ten-year horizon.”

BlueFlag Security · EU Cyber Resilience Act & the SDLC

Be report-ready before 11 September.

See it in under 30 minutes — no agent, no code changes
blueflagsecurity.com

Informational solution brief — not legal advice. References: Regulation (EU) 2024/2847 (Cyber Resilience Act), published OJ L 20 Nov 2024, in force 10 Dec 2024; timeline and reporting mechanics per the European Commission’s CRA implementation and reporting pages and ENISA Single Reporting Platform guidance (notified-body chapter applicable 11 Jun 2026; Art. 14 reporting from 11 Sep 2026; full application 11 Dec 2027; final reports within 14 days for exploited vulnerabilities and one month for severe incidents). Product classification (Annexes III/IV), conformity assessment, CE marking and authority reporting remain customer responsibilities. BlueFlag capability statements reflect public product documentation.