Navigating the

EU Cyber Resilience Act

What organizations need to know — and how X-DLM™ gets you ready

SIEMENS x BLACKDUCK

Powered by Siemens Polarion Application Lifecycle Management and Black Duck Application Security

2.5%	Sept 2026	Dec 2027
Global revenue penalty *for non-compliance*	**Vulnerability reporting** *obligations begin*	**Full enforcement** *deadline*

What is the EU Cyber Resilience Act?

The EU CRA establishes mandatory cybersecurity requirements for all **Products with Digital Elements (PDEs)** sold in the EU/EEA — regardless of where the manufacturer is headquartered or where the product is built. If your product connects to a network and you sell it in Europe, CRA applies to you.

Who it targets	What it governs	Key deadlines	Non-compliance
All producers of software-containing products sold in EU/EEA — globally, not just EU companies.	AppSec risk management, secure-by-design development, vulnerability handling & SBOM generation.	**Effective: Dec 2024** **Reporting: Sept 2026** **Full enforcement: Dec 2027**	Up to 4% global revenue. False statements: 2.5%. Plus EU market exclusion.

Excluded sectors (covered by sector-specific regulation instead)

Medical devices (MDR/IVDR) — Vehicle & aviation safety — National security — Non-commercial OSS — Pure SaaS (no PDE data processing)

Note: CRA exclusions are NOT X-DLM™ disqualifiers. Medical, automotive, aerospace, and industrial sectors operate under equivalent regulations (IEC 62304, ISO 21434, DO-178C, IEC 62443) that Polarion ALM and Black Duck address with equal effectiveness.

Product Classification Determines Your Conformity Path

DEFAULT	IMPORTANT — Class I & II	CRITICAL
Any networked product not in other categories Self-assessment (Module A)	**Auth systems, VPNs, browsers, OSes, routers, wearables, firewalls, hypervisors** Harmonized standards + notified body	**Meter gateways, secure crypto-processors, advanced security systems** Full quality assurance (EUCC)

EU CRA Timeline & Key Obligations

Short timelines demand immediate action. The clock is running regardless of where you are in your compliance journey.

Dec 2024 CRA Effective	Dec 2025 Technical requirements published	Sept 2026 Vulnerability reporting obligations begin	Dec 2027 Full enforcement — all requirements
Scope & classify all products. Map your portfolio against CRA categories.	Gap analysis & SBOM readiness. Identify and close compliance gaps.	**Vulnerability reporting is LIVE. 24h/72h/14-day timelines are now enforceable.**	CE marking, conformity assessment, and full secure-by-design required for EU market access.

! Sept 2026 — Don't miss this

Vulnerability disclosure obligations to CSIRT/ENISA are already active. You must notify actively exploited vulnerabilities within 24 hours of awareness, submit a full exploit report within 72 hours, and deliver a mitigation plan within 14 days. X-DLM BDSCA monitors EUVD continuously — new records processed in under 4 hours.

! Act now — Dec 2027 is closer than it looks

CE marking, SBOM provision, conformity assessments, and full secure-by-design processes all require significant lead time — typically 12–18 months for complex product portfolios. Plan tooling, process, and assessment budgets now to avoid costly late-stage remediation. Contact the X-DLM team to start your scoping assessment today.

5 Essential EU CRA Requirements

Obligations for all manufacturers placing products on the EU market. X-DLM™ addresses all five.

1	**Security by Design & Default**	Products must be designed, developed, and produced with appropriate cybersecurity. Ship without known exploitable vulnerabilities. Secure-by-default configurations required. **X-DLM:** Black Duck SCA detects 3rd-party component vulnerabilities; Coverity flags proprietary code flaws; Defensics validates secure-by-default behaviour.
2	**Vulnerability Handling & Reporting**	Continuous monitoring, regular testing, prompt remediation. Report actively exploited vulnerabilities to CSIRT within 24 hours. Coordinated vulnerability disclosure policy required. **X-DLM:** BDSCA EUVD monitoring with sub-4-hour response; Polarion ALM tracks all issues with full audit trail, timestamps, and automated workflow triggers.
3	**SBOM Provision**	Machine-readable SBOM in SPDX or CycloneDX format covering all direct dependencies. Identify and document all components throughout the product lifecycle. **X-DLM:** BDSCA auto-generates SBOMs in SPDX and CycloneDX; Polarion synchronises SBOM data across the lifecycle, enabling full component and VEX traceability.
4	**Conformity Assessment & CE Marking**	Self-assessment for Default class. Notified body required for Important/Critical. Provide technical documentation and EU Declaration of Conformity. **X-DLM:** Polarion automates technical documentation; SRM consolidates evidence from 150+ security testing tools; X-DLM generates the CE marking evidence package.
5	**Post-Market Surveillance**	Monitor for new vulnerabilities throughout the product lifespan (minimum 5 years). Provide security updates. Communicate unpatched vulnerabilities transparently to customers. **X-DLM:** BDSCA continuously monitors EUVD — new vulnerability records processed in under 4 hours; Polarion Lifecycle Management maintains traceability from concept through EOL.

How X-DLM™ Delivers CRA Conformity

Black Duck SCA integrated into Siemens Polarion ALM — one unified compliance pipeline, built on best-in-class platforms.

Black Duck SCA	Siemens Polarion	X-DLM™ Integration	CRA Conformity
• 3rd-party vulnerability detection • SBOM in SPDX/CycloneDX • EUVD monitoring (<4h response) • License compliance • VDR & VEX generation • Binary & AI code scanning • Malware detection (unique)	• End-to-end lifecycle traceability • Automated technical documentation • Requirements ↔ code ↔ test traceability • Vulnerability impact analysis • Functional safety templates	• Unified compliance dashboard • Automatic SBOM sync & enrichment • Cross-product where-used view • Bespoke remediation workflows • CRA-specific policy enforcement	• CE marking evidence package • EU Declaration of Conformity • Audit-ready report generation • Continuous post-market monitoring **• Sept 2026 reporting ready**

CRA Conformity Steps with X-DLM™

From applicability assessment to continuous monitoring — X-DLM™ supports every phase.

1 Applicability Assessment

Determine if and how the CRA applies to your products and organisation. X-DLM experts guide scoping against product classification tiers. This step is a Legal/GRC action, not a development team decision.

2 Product Classification

Classify each product as Default, Important (Class I or II), or Critical. Classification drives your conformity path, CE marking requirements, and the level of third-party assessment required.

3 Gap Analysis & Risk Assessment

Assess existing AppSec processes against CRA essential requirements. Polarion connects vulnerabilities to components, requirements, and remediation actions. Identify whether you can produce an SBOM and hit the 24-hour reporting window today.

4 Technical Documentation

Prepare SBOMs, VDRs, VEX artefacts, test reports, and user instructions. Polarion automates traceability across all artefacts. X-DLM maintains the documentary chain from design through to release.

5 Conformity Assessment & CE Marking

Carry out your chosen conformity procedure — self-assessment (Default) or notified body (Important/Critical). SRM consolidates evidence from 150+ security tools. X-DLM generates the CE marking package automatically.

6 **Continuous Monitoring & Post-Market Surveillance**

Vulnerability reporting obligations are active from September 2026. BDSCA monitors EUVD continuously — new records processed in under 4 hours. Polarion maintains full lifecycle traceability through end-of-life (minimum 5 years).

Budget note: CRA obligations require sustained investment through December 2027. Plan tooling, process, and assessment budgets now to avoid costly late-stage remediation.

Business Impact at Scale

CRA conformity is not just a compliance obligation — it is a competitive advantage. Organizations that demonstrate governed security decisions and lifecycle transparency turn compliance into a measurable growth accelerator.

60–80%	**10–20%**	**20–25%**	**25%+**
reduction in audit prep time	**increase in delivery velocity**	**fewer engineering hours on compliance**	**reduction in legal & certification workload**
Weeks of manual effort become hours of automated output	Automated workflows eliminate manual compliance bottlenecks	Governed automation replaces ad-hoc manual processes	Pre-built regulator-ready documentation reduces review cycles

Book a Demo

See how X-DLM™ connects Black Duck's best-in-class SCA intelligence with Siemens Polarion's lifecycle governance — automating SBOMs, vulnerability workflows, 24h reporting, and audit-ready evidence across your entire product lifecycle.

Liv Valdez | Business Development

+1 647-228-3070 | liv@electrosource.com

x-dlm.com