cloudsmith

Is your software supply chain ready for the EU Cyber Resilience Act?

The EU Cyber Resilience Act sets mandatory cybersecurity requirements for any manufacturer placing software products on the EU market regardless of where your company is based. The first hard deadline is **11 September 2026,** when reporting obligations take effect. Full enforcement begins in December 2027.

This checklist helps you assess how your current engineering and security practices map to the CRA's core requirements for the software supply chain layer. The goal is to identify where you're already well-positioned and where there's work to do.

1. Component visibility

Do you have a complete, current record of every open-source and third-party component in your products, including transitive dependencies?

The CRA requires manufacturers to identify and document all components in a machine-readable Software Bill of Materials (SBOM), covering at minimum top-level dependencies (Annex I Part II, point 1).

☑	Yes	We generate SBOMs automatically for every build, in a machine-readable format, and they stay current as dependencies change.
☐	Partially	We generate SBOMs, but the process is manual, tied to release cycles, or doesn't cover all products or dependency layers.
☐	No	We don't have a consistent SBOM process in place.

2. Vulnerability monitoring

Do you have a process for detecting newly disclosed vulnerabilities in components already in your products and not just at the point they were added?

The CRA requires ongoing vulnerability tracking throughout the product's support period, not point-in-time scanning (Article 13(7), Annex I Part II, point 3).

☐	Yes	Vulnerability data feeds update continuously against our artifact inventory. New disclosures are matched to existing packages automatically.
☐	Partially	We scan at ingestion or on a schedule, but don't have automated re-evaluation when new CVEs are disclosed against packages already in our registry.
☐	No	Vulnerability scanning is ad hoc or happens only at release.

3. Exploitability assessment

When vulnerabilities are identified, can you distinguish between those that are theoretically present and those that are realistically exploitable in your product?

The CRA prohibits shipping products with known exploitable vulnerabilities — meaning vulnerabilities that can be effectively used by an adversary under practical conditions (Article 3(41), Annex I Part I, point 2(a)).

☐	Yes	We enrich CVEs with exploitability data (such as EPSS scores) and use that to prioritize remediation and gate releases.
☐	Partially	We use severity scores (CVSS) but don't assess realistic exploitability in our specific environment.
☐	No	We treat all CVEs the same or don't have a structured triage process.

4. Supply chain control

Do you have an enforced control layer between public package registries and your build pipelines?

The CRA requires manufacturers to exercise due diligence over third-party and open-source components before they enter products (Article 13(5), Annex I Part I, point 2(j)).

☐	Yes	All dependencies pass through a governed proxy with automated policy enforcement before reaching developer machines or pipelines. Developers cannot pull directly from public registries.
☐	Partially	We have some controls in place, but enforcement is inconsistent across teams, formats, or environments.
☐	No	Developers pull dependencies directly from public registries without a consistent checkpoint.

5. Incident reporting readiness

If you learned today that a vulnerability in one of your products was being actively exploited, could you file a structured report with EU authorities within 24 hours?

From 11 September 2026, Article 14 requires an early warning notification within 24 hours of becoming aware of an actively exploited vulnerability, a full notification within 72 hours, and a final report within 14 days of a corrective measure being available.

☐ Yes	We have defined internal workflows, the necessary audit trail, and immediate visibility into affected components to support all three reporting windows.
☐ Partially	We could assemble the information, but it would require manual effort across multiple teams and tools — and we're not confident we'd meet the 24-hour window.
☐ No	We don't have the detection infrastructure or internal process to respond within the required timeframes.

6. Access control

Can you demonstrate that access to your software supply chain infrastructure follows least-privilege principles and that access is revoked promptly when people leave?

The CRA requires appropriate access controls as part of secure-by-design principles (Annex I Part I, point 2(d)).

☐ Yes	We have role-based access control, SSO enforcement, and automated provisioning/deprovisioning tied to our identity provider.
☐ Partially	Access controls exist but are managed manually, inconsistently applied, or not systematically reviewed.
☐ No	Access management is informal or not consistently enforced across our artifact infrastructure.

7. Audit trail

Do you have a complete, tamper-evident record of who accessed, uploaded, modified, or deleted artifacts in your software supply chain that is exportable on demand?

The CRA requires manufacturers to maintain evidence of their security practices and produce it for market surveillance authorities on request (Article 13(13), Annex I Part I, point 2(l)).

☐ Yes	All artifact activity is logged immutably, accessible via API, and exportable to our SIEM or monitoring tools.
☐ Partially	Some logging exists but it's incomplete, scattered across tools, or not readily exportable in a usable format.
☐ No	We don't have a centralized, reliable audit trail for artifact activity.

How to read your results

Scoring: Yes = 2 points | Partially = 1 point | No = 0 points

12–14 points: Strong foundation

Your practices are broadly aligned with what the CRA requires. The priority now is closing any remaining gaps and making sure your processes are documented and defensible because demonstrating compliance matters as much as achieving it. Use this checklist as a baseline for your compliance review and identify any "Partially" answers as your next focus area(s).

7–11 points: Work in progress

You have meaningful controls in place, but there are gaps that need to close before September 2026. The areas where you answered "Partially" or "No" represent real compliance risk, particularly around reporting readiness and vulnerability monitoring, which have the earliest deadlines. Prioritize those first, then work through the structural gaps in supply chain control and audit infrastructure.

0–6 points: Start now

You have meaningful controls in place, but there are gaps that need to close before September 2026. The areas where you answered "Partially" or "No" represent real compliance risk, particularly around reporting readiness and vulnerability monitoring, which have the earliest deadlines. Prioritize those first, then work through the structural gaps in supply chain control and audit infrastructure.