activestate

# CRA Readiness Assessment:
# 5 Questions for Engineering Leaders

*This diagnostic maps to CRA Article 13 and Article 14 obligations as currently understood. It is not legal advice. Consult your legal team to confirm scope and applicability for your specific products and business model.*

CRA creates the first product-level cybersecurity liability most organizations have ever faced. These are five questions to help you unearth specifics that the regulations encompass, and that your team needs to be able to answer.

## Question 1 — If you build OSS governance internally, what does that actually cost?

- [ ] How long would it take your team to build and maintain a governed OSS inventory across every language ecosystem you ship, and keep it current as dependencies change?
- [ ] Does your current tooling cover the full CRA requirement, including machine-readable SBOM covering transitive dependencies, validated provenance, and defined remediation SLAs, or just part of it?
- [ ] Who owns OSS governance on your team, and do they have the capacity to maintain it alongside existing roadmap commitments?
- [ ] What's the timeline to have this operational before regulation dates, and does it fit inside your H2 roadmap?

**14% of developer time already goes to security work (GitLab/Harris Poll, 2024). CRA adds process, documentation, and reporting overhead on top of that. The build path is slower than it looks on a roadmap.**

## Question 2 — Can your team map a CVE to every affected product within hours?

- [ ] That's what the 24-hour reporting window requires.
- [ ] When a CVE drops, how long does it take your team to know which products are affected, which versions, and which customers are at risk?
- [ ] Does your SBOM cover transitive dependencies, or just direct ones? 64% of OSS components in production are transitive (Black Duck OSSRA). If your inventory stops at direct dependencies, it stops before most of your risk.
- [ ] Is your SBOM current as of this week, or as of your last release?
- [ ] Do you know the provenance of every OSS component in your stack, including where it came from, what version, and under what license?

**The average MTTR in the software industry is 55 days (Edgescan 2026). CRA's reporting window starts at 24 hours. That gap is unlikely to close through process alone.**

activestate

## Question 3 What does CVE remediation actually cost your team right now?

- [ ] How many CVEs does your team remediate per quarter, and how long does each one take?
- [ ] At 4-8 developer hours per CVE remediation (Chainguard/Hopper poll), what's the total engineering cost annually?
- [ ] How much of that cost comes from chasing transitive dependencies your team didn't know existed until a CVE surfaced them?
- [ ] When CRA requires a documented record of every remediation decision, not just the fix, what does that add to your team's workload?

**98% of applications include open source (Black Duck OSSRA). An ungoverned OSS layer isn't a niche problem. It's the engineering resourcing inside every product you ship.**

## Question 4 Could your team produce an audit trail for any CVE remediation in the last 12 months?

This is the question a regulator will ask. It's worth asking yourself first.

- [ ] Do you have a documented record of when you became aware of each CVE, what was affected, what you did, and how long remediation took?
- [ ] Are your remediation SLAs for critical and high CVEs documented and enforced, or informal and aspirational?
- [ ] If a market surveillance authority asked for your vulnerability handling records tomorrow, how long would it take to produce them, and how confident are you in what they'd show?
- [ ] Are your developers pulling from public registries directly, or do you have a governance layer between the registry and your build pipeline?

**CRA requires a vulnerability handling process that can survive an audit, covering intake, triage, remediation, and disclosure, with defined owners at each stage. If it can't produce a paper trail on demand, it won't hold up.**

activestate

## Question 5 — Who owns this, and have you confirmed that with your CISO?

- [ ] Is there a named owner for CRA readiness who sits across both security and engineering?
- [ ] Has your CISO confirmed which products are in scope and what the engineering mandate actually is?
- [ ] Does your team have defined trigger criteria for the 24-hour early warning, 72-hour full notification, and 14-day final report, or is that still sitting with the security team?
- [ ] If a CVE dropped tonight, would your team know immediately what their role in the response is?

**Ownership ambiguity is the most common reason engineering teams with good intentions miss hard deadlines. CRA creates a split obligation. Security owns the compliance requirement, engineering owns the implementation. Without a named owner bridging both, CRA will find that gap.**

# Where Does Your Team Stand?

- **Answered confidently across all five:** Stronger than most. Focus on closing remaining gaps, testing your reporting pipeline end-to-end before regulation due dates, and confirming SBOM coverage is current across all in-scope products.
- **Struggled with two or three:** Critical gaps remain, likely in transitive dependency coverage, remediation plans, or ownership clarity. Regulatory standing is at risk without action in the next 60 days.
- **Couldn't answer most of them:** Gaps are structural. Building the required infrastructure from scratch while maintaining roadmap velocity is unlikely to be possible within the next three months.

Talk to an expert about where your organization stands →