THE LINUX FOUNDATION | Research

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

balena ERICSSON REVANITE

2026 CRA Awareness and Readiness

Structural Unreadiness and Stagnating Awareness for Global CRA Compliance, And the Time-bound Need to Close the Gap

Adrienn Lawson, The Linux Foundation

Foreword by Roman Zhukov, Red Hat

June 2026

2026 CRA Awareness and Readiness

66% of respondents remain unfamiliar with the CRA, similar to the level in 2025 (62%), despite the regulation entering into force during the year.

72% of US and Canadian respondents are unfamiliar with the CRA, despite needing to comply if selling products into the EU market.

41% of organizations already familiar with the CRA have still not determined whether the regulation actually applies to them.

Only 34% of respondents correctly identify December 2027 as the full compliance target year, while 46% remain uncertain about deadlines altogether.

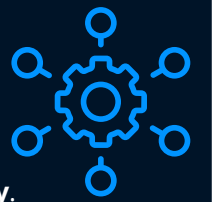
56% of respondents are unaware that **non-compliance fines can reach €15 million or 2.5% of global annual turnover**.

Only 32% of manufacturers produce SBOMs for all products, and 51% still passively rely on upstream projects for security fixes.

Maintaining an average of 86 private forks costs organizations approximately $258,000 in labor every release cycle, which greatly scales with organization size.

Only 41% of manufacturers expect to be fully compliant by December 2027, while 39% do not know when they will be.

Analysis of 12,863 projects shows the number of contributing organizations strongly predicts a project's security posture, **making upstream investment a direct compliance strategy**.



48% learned about the CRA through digital media and developer communities; official EU channels reached only 25% of respondents.

59% of non-commercial OSS developers say **clear guidance on their CRA status would reassure them about continuing to contribute**.

CVE discoveries surged 394% year-over-year in Q1 2026, with high-severity vulnerabilities up 811% across 14,000+ open source projects.

Table of Contents

Foreword

As a co-chair of the OpenSSF Global Cyber Policy Working Group and a Red Hat representative at European Standardization Organizations (ESOs), I have a front-row seat to the open source community's evolving relationship with the European Cyber Resilience Act (CRA).

In previous years, OpenSSF's mission focused heavily on education and navigation, helping the community and industry understand what this landmark regulation meant for different entities, while actively influencing and supporting European standardization efforts. Through continuous mapping of compliance pathways and conducting productive workshops, we laid crucial groundwork and achieved good results: open source is finally viewed as a critical piece of technology that all CRA manufacturers rely on.

This year, however, we must pivot. We need to channel our energy into practice, focusing on how we can implement the CRA's requirements in the most meaningful and sustainable way for everybody. A cornerstone of this practical implementation is embracing the principles of shared responsibility as the only way towards a more secure and sustainable ecosystem that the entire world runs on. As highlighted in multiple Red Hat publications, organizations that consume open source must partner with projects to adopt pragmatic, developer-centric security hygiene that is beneficial for everyone.

Yet, as we make this push toward practical implementation, the 2026 CRA Awareness and Readiness Report reveals a sobering truth: while our policy frameworks are fairly mature, the broader ecosystem's readiness is far from perfection. With the September 2026 reporting obligations just months away and the December 2027 full enforcement deadline approaching, this data must serve as a wake-up call. Shockingly, 66% of respondents remain unfamiliar with the CRA. Even more concerning is the structural unreadiness among manufacturers. With 51% of organizations still passively relying on upstream projects for security fixes, the traditional model of "consume and forget" is fundamentally incompatible with the CRA's mandate for active due diligence.

The report highlights the staggering technical debt created by compliance workarounds: organizations maintaining private forks are burning an average of $258,000 per release cycle. Although it's still uncertain how to navigate CRA compliance for manufacturers, one thing is clear: investing in the diversity and security of the open source projects you depend on is no longer just good citizenship - it is an essential part of doing business.

I strongly urge developers, manufacturers, and stewards to read this report closely. Awareness alone is insufficient. CRA is by nature different from any other compliance frameworks we have seen before. Abandon unsustainable private forks, step up to the standardization table, and join us in building a more secure global software supply chain.

Roman Zhukov

Security Communities Lead, Red Hat Open Source and AI Program Office
Co–Chair, OpenSSF Global Cyber Policy Working Group

Executive summary

The 2026 CRA Awareness and Readiness Report assesses how the global software ecosystem is preparing for the **European Cyber Resilience Act (CRA)**. Building on the 2025 study, **Unaware and Uncertain: The Stark Realities of Cyber Resilience Act Readiness in Open Source**, this year's research incorporates a larger sample of 843 respondents, a 23% increase from the previous year, alongside a security analysis of over 12,000 open source projects. The findings show stagnating awareness and structural unreadiness as the December 2027 full compliance deadline draws near.

The most significant finding of the 2026 survey is the lack of improvement in industry-wide awareness. Despite the CRA entering into force, the proportion of respondents who are either not familiar at all or only slightly familiar with the regulation rose to 66%. This awareness dip may be attributed to the survey's broader reach into new audiences, particularly in the United States and Canada, where unfamiliarity is at 72%. Given that any organization placing commercial products on the EU market must comply, this geographic disparity suggests a major segment of the global supply chain remains materially unprepared. Even among those aware of the CRA, understanding has not deepened, with 41% of organizations still having not determined if the regulation applies to them. Furthermore, 46% are uncertain about compliance deadlines—with only 34% correctly identifying 2027 as the target year—while 56% are unaware of the penalties for non-compliance. Many organizations also continue to struggle with core definitions, as 54% are still working to distinguish between the roles of manufacturers and stewards, which carry different regulatory obligations.

Manufacturer readiness remains largely static, as only 32% produce Software Bills of Materials (SBOMs) for all products and 51% continue to rely passively on upstream projects for security fixes. A critical new data point highlights the economic burden of private forking as a compliance workaround; on average, organizations maintain 86 private forks, costing approximately $258,000 in labor per release cycle. For large organizations (5000+ employees), this burden exceeds 11,000 labor hours per cycle, suggesting the CRA may ultimately force a shift toward upstream contribution as the only financially rational path forward. Small and medium-sized enterprises are simultaneously the most exposed as 62% rely on open source for more than three quarters of their products, compared to 35% in larger organizations. Currently, 51% of European small and medium-sized enterprises remain unfamiliar with the CRA, and 47% of manufacturers in this segment expect to raise prices to cover compliance costs.

Data from over 12,000 open source projects indexed on LFX reveals a 394% year-over-year surge in published CVEs in Q1 2026, with high-severity findings up 811%. Likely causes for this increase could include improved automated scanning, analysis by AI-based tools, or CRA-prompted auditing. This scale of growth points to an expanding visibility into the realities of the vulnerability burden across the components manufacturers depend on.

The LFX data also points to what makes some projects more resilient than others. Organizational diversity is a strong predictor of security, meaning that investing in upstream projects is a direct investment in a manufacturer's own compliance posture. To bridge the readiness gap, the ecosystem must move from policy analysis to operational toolkits, such as automated compliance tools and clearer guidance for the 61% of non-commercial developers who are currently unsure of their status under the CRA. Financial and legal support for stewards is also essential to manage rapid vulnerability response. Ultimately, success will require moving beyond official regulatory channels to community-driven spaces, such as open source foundations, online discussions, and social media, where the majority of practitioners learn and collaborate.

Introduction

The CRA is a landmark piece of European cybersecurity regulation. It covers a wide range of products, essentially any hardware or software capable of connecting to a device or network. This spans everything from smart home devices and consumer apps to industrial sensors, enterprise software, and connected vehicles, making it relevant to the vast majority of technology products on the market. While it includes important exemptions for non-commercial free and open source software development, it creates significant new obligations for manufacturers, as well as for importers and distributors, in the commercial supply chain. In contrast, open source software (OSS) stewards are subject to a lighter regulatory regime, with comparatively limited obligations.

The CRA provides great momentum to fix security practices in open source projects that had previously been neglected. This is the optimistic reading of the regulation's impact: it incentivizes a long-overdue shift in how manufacturers engage with the open source communities they depend on. The pessimistic reading is that the transition is happening too slowly. Without action, manufacturers risk being caught unprepared at enforcement, while the open source projects they depend on could face unsustainable pressure.

The 2026 survey was conducted in early 2026 with a sample of 843 respondents, drawn from Linux Foundation subscribers, partner communities, and social media. Respondents spanned the software industry across geographies, organization sizes, and industry sectors. The methodology mirrors the 2025 study to allow year-on-year comparison.

The survey included a general awareness section (n=843) plus role-specific modules for manufacturers (n=194–219), stewards (n=28), and a non-commercial open source section (n=109).

Note on the steward sample: The steward sample (n=28) is smaller than in 2025 (n=34). Findings from this segment are directionally informative but should be interpreted with appropriate caution given the limited sample size.

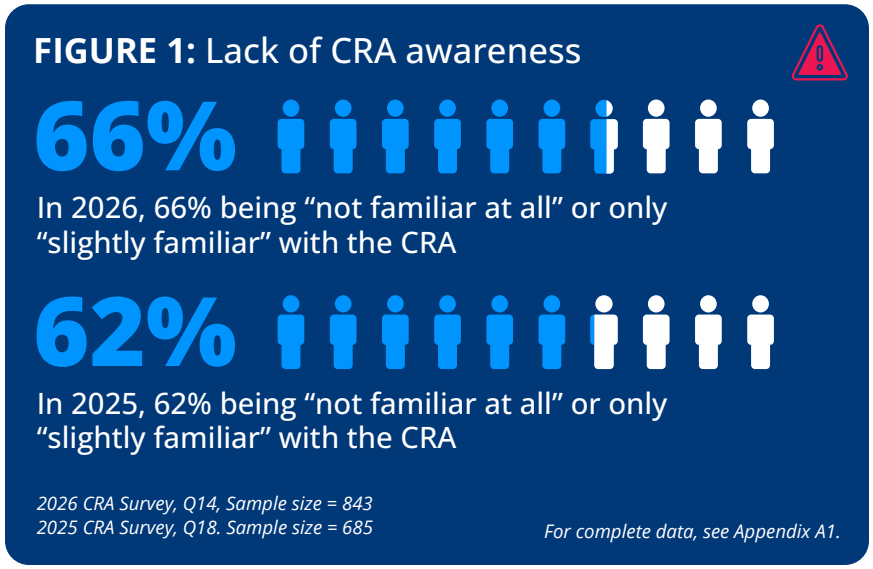
Stagnating low awareness

Overall awareness has not improved

The most important top-line finding of the 2026 survey is the lack of improvement in awareness as shown in **FIGURE 1**. Between January 2025 and January 2026, during which the CRA entered into force and the community launched various education and awareness initiatives, the proportion of respondents who are either "not familiar at all" or only "slightly familiar" with the CRA has increased from 62% to 66%.

One plausible explanation of this finding is that the 2026 sample includes more respondents overall, therefore the reach of the audience went further and includes those we did not reach last year. It may be that other topics, especially the rise of AI, have garnered so much attention that other issues like the CRA have been drowned out. It may also be that IT has historically never been regulated this way, so the IT community simply never looks for nor considers the impact of regulatory changes. There are likely other factors at play too but regardless of cause, the aggregate signal is clear: overall industry-wide awareness has not improved in the past year.

FIGURE 1: Lack of CRA awareness



2026 CRA Survey, Q14, Sample size = 843
2025 CRA Survey, Q18. Sample size = 685

For complete data, see Appendix A1.

As **FIGURE 2** shows, regional awareness continues to follow predictable patterns, with European respondents showing higher familiarity than their counterparts in North America and Asia-Pacific. Understanding differences in regional awareness is important given the global nature of software supply chains. Any organization placing products on the EU market, including North American and Asia-Pacific companies, must comply with the CRA. An unfamiliarity rate of 72% among US and Canadian respondents means that the majority of North American companies selling software in Europe may be materially unprepared for the September 2026 reporting deadline. This is the CRA's earliest compliance deadline for most, which requires manufacturers to report actively exploited vulnerabilities and severe security incidents.

Under the CRA: Compliance timeline

In plain terms, the CRA rolls out in three stages (**CRA, Recital 126**):

- **11 June 2026:** Entry into application of the provisions on the notification of Conformity Assessment Bodies. Member States to designate notifying authorities (**CRA implementation document**)
- **11 September 2026:** Manufacturers must begin reporting actively exploited vulnerabilities and severe security incidents
- **11 December 2027:** The Regulation applies in full

For most manufacturers, September 2026 is the first deadline that demands action.

FIGURE 2: Regional unfamiliarity

How familiar are you with the Cyber Resilience Act (CRA)? (select one)

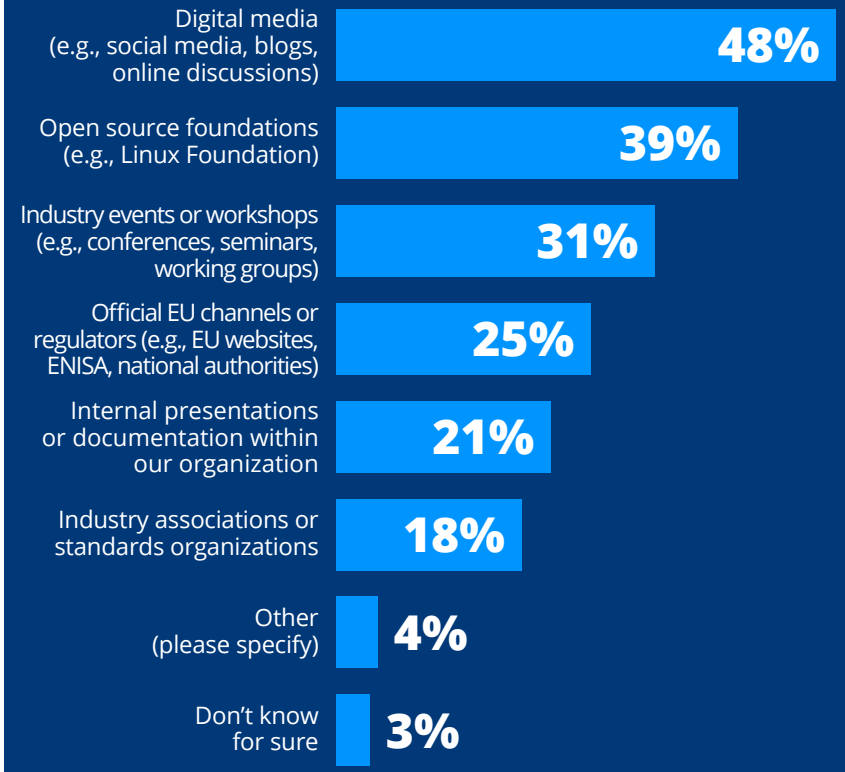
2026 CRA Survey, Q14 by Q4, Sample size = 718

For complete data, see Appendix A2.

Crucially, as **FIGURE 3** shows, 48% of respondents who learned about the CRA did so via digital media (social media, blogs, online discussions), and 39% via open source foundations. Official EU channels reached only 25% in our sample. This suggests the most effective awareness channels are community-driven, especially for people in technical positions. The role of foundations as information intermediaries deserves emphasis, though the sample skews toward practitioners already engaged with open source governance, a limitation worth bearing in mind when generalising the findings.

FIGURE 3: Channels for learning about the CRA

Where did you learn about the CRA? (select all that apply)



2026 CRA Survey, Q16, Sample Size = 404, Total Mentions = 767

Action: Outreach through community channels

Because digital media and open source foundations are important awareness channels, a high ROI investment for the support ecosystem is content that travels in developer spaces: short-form explainers, conference talks, podcast appearances, and integration of CRA guidance into popular OSS tooling documentation. Formal EU communication alone has not been sufficient.

Specific knowledge gaps

Beyond the general lack of awareness, the 2026 survey reveals that specific knowledge gaps among CRA-aware respondents have also remained largely static from last year's survey. This is another significant finding: even among those who have heard of the CRA, understanding has not deepened.

Among respondents who reported some familiarity with the CRA, several critical knowledge gaps emerged similar to last year (**FIGURE 4**). We found that 41% of organizations have not yet determined whether the regulation applies to them. This uncertainty could lead to significant compliance challenges as implementation deadlines approach.

The survey also revealed that 46% of respondents are uncertain about compliance deadlines, with only 34% correctly identifying 2027 as the target year for full compliance. Furthermore, 56% of respondents indicated that they are unaware of the penalties for non-compliance, suggesting a critical need for education about the regulation's enforcement mechanisms.

It appears that respondents are also still uncertain of distinction between the roles of manufacturers and stewards under the CRA, representing another key area for knowledge development. Currently, 54% of respondents are working to understand these classifications, confirming the need for creating clear frameworks and guidelines to help organizations accurately determine their roles and corresponding obligations.

Under the CRA: Penalties for non-compliance

"The penalties provided for shall be effective, proportionate and dissuasive." (**CRA, Article 64(1)**)

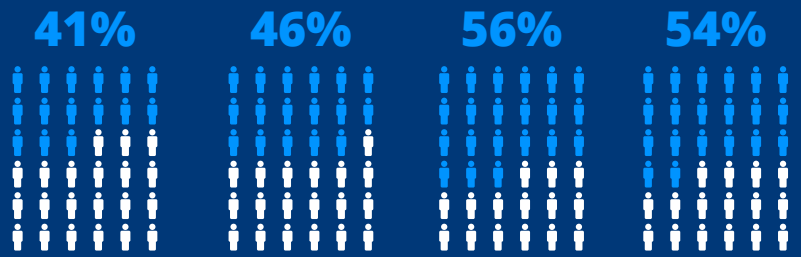
When determining the fine amount, authorities must consider the nature, gravity and duration of the infringement, whether previous fines have been applied, and the size of the offending organisation.
Fines are tiered by the nature of the infringement:

- **Non-compliance with essential cybersecurity requirements:** Up to €15,000,000 or 2.5% of global annual turnover (whichever is higher)
- **Non-compliance with other obligations:** Up to €10,000,000 or 2% of global annual turnover for non-compliance with other obligations
  - Other obligations are laid out in Articles **13** & **14**
- **Supplying incorrect or misleading information to authorities:** Up to €5,000,000 or 1% of global annual turnover

Exemptions **(CRA Article 64(10)):**

- Microenterprises and small enterprises are exempt from fines for missing the 24-hour early warning notification deadline
- Open source software stewards are exempt from fines for any infringement of the Regulation

FIGURE 4: Findings from CRA-aware respondents, with no significant change from last year



2026 CRA survey, Q20, Q18, Q21,Q19, Sample size = 404

For complete data and a comparison with 2025, see Appendix A3-A6.

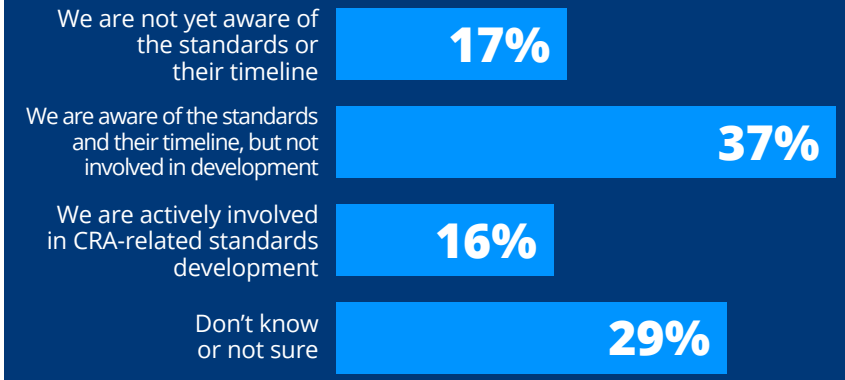
Standards development

One of the 2026 survey's new data points concerns awareness of and involvement in CRA-related standards development. The CRA relies heavily on harmonized European and international standards to define, among other things, what "secure by design" means in practice. Without these standards, organizations face interpretive uncertainty about what compliance requires in practice.

This matters because the development of harmonized standards under CRA Article 19 will directly determine the compliance pathways available to manufacturers. Organizations engaged in standards work will have informational advantages, and may have opportunities to shape requirements. As shown in **FIGURE 5**, the 46% who are unaware or unsure of standards timelines and their involvement, and the 37% who are aware but uninvolved, risk being confronted by finalized standards they had no hand in crafting, no awareness of their consequences, and little time to implement.

FIGURE 5: 46% of organizations not aware of standards development

What is your organization's involvement with CRA-related standards? (select one)



2026 CRA Survey, Q22, Sample size = 194

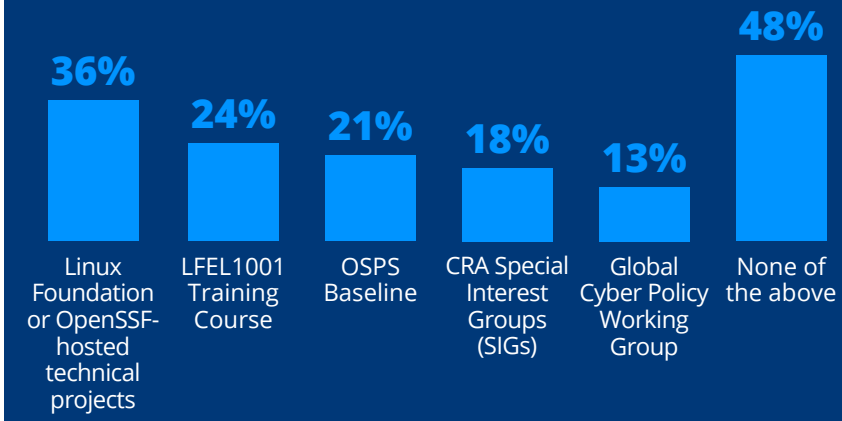
Awareness of widely available tools is low

A rich set of CRA resources exists, yet awareness remains a significant challenge across the community that we investigated (**FIGURE 6**). We focused on Linux Foundation and OpenSSF CRA-related initiatives, though we acknowledge that other resources exist too, but were not part of our study. The results show that 48% of respondents were unaware of any Linux Foundation or OpenSSF CRA-related initiative, highlighting a substantial discoverability gap (**FIGURE 6**). Among those who were aware, Linux Foundation or OpenSSF-hosted technical projects had the

highest recognition at 36%, followed by the **LFEL1001 Training Course** at 24% and the **OSPS Baseline** at 21%. Awareness drops further for more specialized resources, with CRA Special Interest Groups (SIGs) known to only 18% of respondents and the Global Cyber Policy Working Group recognized by just 13%.

FIGURE 6: Awareness of CRA initiatives (LF and OpenSSF)

Are you aware of the following CRA-related initiatives from the Linux Foundation and OpenSSF? (select all that apply)



2026 CRA Survey, Q23, Sample size = 396, Total mentions = 634

As shown in **FIGURE 7**, all five initiatives received average usefulness scores between 3.78 and 4.19 on a scale of 1 to 5, which shows the clear helpfulness to those who come across their contents. The **LFEL1001 course** in particular represents a high-value, zero-cost resource: free, 60 to 90 minutes, and rated 3.78/5. Yet only about one in three respondents knows it exists (**FIGURE 6**). This suggests that there needs to be new ways to make others aware of these resources; good resources only help those aware of them.

FIGURE 7: Awareness of CRA initiatives (LF and OpenSSF)

Please rate how useful you found these initiatives. (select one response per row)

Initiative	Average usefulness score (1 - Not useful, 5 - Essential)
OSPS Baseline	3.91
LFEL1001 Training Course	3.78
CRA Special Interest Groups (SIGs)	3.93
Global Cyber Policy Working Group	3.92
Linux Foundation or OpenSSF-hosted technical projects	4.19

2026 CRA Survey, Q24, Sample size = 81, 94, 69, 51, 141

We also received open-text responses to what support doesn't exist but should, which reveal a clear demand signal (**FIGURE 8**). The most cited asks are not more policy analysis or white papers on the CRA, but practical, step-by-step operational guidance, especially for smaller organizations.

Action: Invest in implementation toolkits

The support ecosystem has produced strong awareness-level materials. As noted above, there needs to be different or more efforts to get the word out to those affected. The next investment priority should perhaps be operational toolkits: CRA compliance checklists by organization size, SBOM generation templates, vulnerability disclosure workflow templates, and annotated examples of security policies that satisfy CRA Article 24 steward requirements. These would address the top-cited support gap across manufacturer, steward, and SME segments.

FIGURE 8: Textual answers for new CRA initiatives

Answers thematically categorized and ranked according to number of mentions.

- **Practical implementation guidance** (~12 mentions) - Real-world workflows, step-by-step guides, mapping to existing standards
- **Educational resources and training** (~10 mentions) - Simplified explanations, online courses, workshops, videos, crash courses
- **SME/small company support** (~8 mentions) - Affordable compliance paths, templates, tooling for resource-constrained organizations
- **Clear documentation and summaries** (~7 mentions) - Plain language guides, TLDR versions, concise overviews, key points
- **OSS-specific guidance** (~6 mentions) - Due diligence frameworks, open source baselines, vulnerability management for OSS
- **SBOM and tooling support** (~5 mentions) - Templates, VDR standards, automation tools, technical frameworks
- **Standard interpretation help** (~4 mentions) - Explanations of horizontal/vertical standards, updates on revisions
- **Financial support mechanisms** (~3 mentions) - Funding for OSS projects, subscription models, affordability solutions
- **Industry-specific guidance** (~3 mentions) - Non-IT sectors (healthcare, chemical), educational institutions
- **Regulatory awareness** (~3 mentions) - Newsletters on policies, enforcement, penalties, insurance implications
- **International cooperation** (~2 mentions) - Academic partnerships, global market compliance guidance

2026 CRA Survey, Q25, Sample size = 60

From the experts

PHIL ROBB
Head of Ericsson Software Technology

ERICSSON

Cambridge Dictionary defines resilience as "*the quality of being able to return quickly to a previous good condition after problems*." In an age of hyper-connected devices and AI-powered threats, cyber resilience is essential.

Ericsson has engaged with the CRA since its 2022 draft, working with regulators to benefit our customers and the open source ecosystem. Since early 2024, we've strengthened many open source projects through CVE fixes, dependency uplifts, SBOMs, automated dependency bumping, and zero-trust hardening.

But bad actors aren't slowing down. That's why companies are uniting at the Open Source Security Foundation. **Join us—resilience is a team sport**.

Manufacturer readiness

Limited change in manufacturer readiness

Manufacturers face a structural choice in how they address their open source software dependencies under the CRA: fork and maintain privately, pay for enterprise support, actively contribute back to upstream communities, or any combination of these activities. The data suggest that many organizations have not yet made this choice, and those that have are disproportionately choosing private maintenance patterns that create technical debt and do not strengthen the broader ecosystem.

Our analysis of manufacturer practices reveals significant gaps in preparation for CRA compliance similarly to last year, as shown in **FIGURE 9**. Only 32% of manufacturers currently produce SBOMs for all of their products. We also found that more than half (51%) of manufacturers passively rely on upstream projects for security fixes. The survey also revealed that only 34% of manufacturers regularly assess the security practices of their OSS components, falling short of the risk management and documentation mandates outlined in the regulation. Looking toward future contributions, 59% of manufacturers remain uncertain about their plans for upstream contributions, while 20% have already decided against increasing their engagement.

In practice: Passively relying on upstream projects

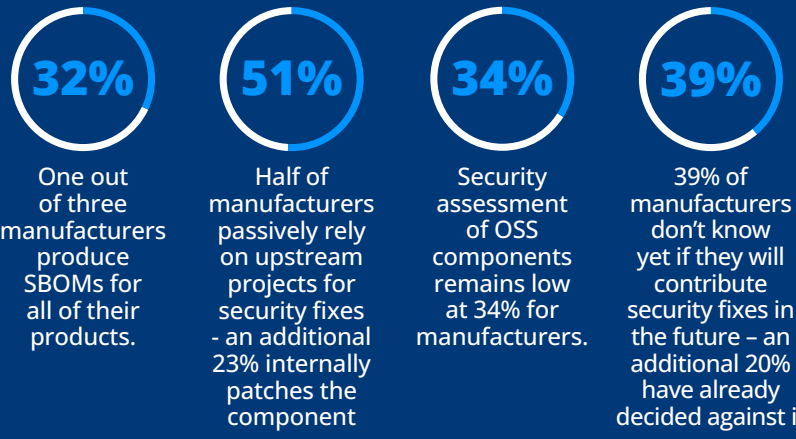
When a manufacturer ships a product that includes an open source component, they are taking on responsibility for the effect of that component on their product's security. Passive reliance means they have no direct relationship with the upstream project. They are not contributing fixes, not monitoring the project's health, and not tracking when vulnerabilities are disclosed. They are simply waiting for a new version to appear and hoping someone else caught the problem first. Under the CRA, that posture is no longer tenable. Manufacturers are required to exercise due diligence when integrating third-party components into their products, and to notify the components' providers about vulnerabilities and developed fixes—including open source components (see **CRA Art. 13(5) and (6)**).

Under the CRA: Manufacturers bear responsibility

The CRA places responsibility for security maintenance squarely on manufacturers who integrate open source components into their products (see CRA **article 13**). The regulation does not impose obligations on non-commercial open source projects to provide rapid security fixes, nor does it expect them to shoulder the burden of commercial users' compliance requirements. Instead, it creates a framework where manufacturers must actively take responsibility for their dependencies' security. The CRA explicitly allows manufacturers to contribute to fixes upstream and provide financial support to open source projects without this being classified as commercial activity (CRA **recital 18**). This presents an opportunity for manufacturers to shift from passive consumption to active participation in the open source ecosystem, whether through direct code contributions, security improvements, or sustainable funding models.

FIGURE 9: Current interaction patterns between manufacturers and their OSS components in use

With no significant changes from last year



2026 CRA Survey, Q28, Q30, Q29, Q34, Sample size = 194-219

For complete data and a comparison with 2025, see Appendix A6-A10.

The cost of forking in the age of the CRA

Private forks can be a short-term workaround for CRA compliance, but the **ROI for Open Source Software Contribution Report** reveals the significant costs this approach imposes at scale. A key insight from the report is that maintaining private forks represents a growing form of technical debt: on average, an organization maintains 86 private forks of open source components, each requiring 60 labor hours for maintenance and integration per release cycle. This means the average organization must dedicate 5,160 labor hours, equivalent to $258,000 USD[1] to maintain private forks every release cycle.

These costs scale sharply with organization size as shown in **FIGURE 10**. Small organizations (1 to 249 employees) require around 147 labor hours per release cycle to maintain private forks, while large organizations (more than 5,000 employees) face over 11,152 hours. This annualized burden represents enormous amounts of engineering time that could otherwise be directed toward innovation or upstream contribution.

The CRA makes these costs harder to ignore. The regulation's requirements around vulnerability handling, security updates, and software transparency create new pressure to maintain a clear, auditable chain of provenance for every component. This is something private forks inherently complicate. Contributing fixes upstream, by contrast, amortizes maintenance costs across the entire user community of a project and eliminates the burden of managing divergent codebases. This would all help in producing the kind of transparent, well-documented software supply chain the CRA demands. While the regulation introduces short-term legal complexity, it may ultimately shift the economics decisively toward upstream engagement and making upstream contribution not just best practice, but the only financially rational path forward. This does not require manufacturers to redirect their entire development effort upstream. It requires only that vulnerability fixes relevant to their product be contributed back, a targeted commitment that remains well within reach of any organisation already maintaining a private fork.

[1] *This cost is the product of (a) the average number of labor hours required to maintain private forks per release cycle from survey responses and (a) an hourly wage of $50 USD, consistent with the median global response by software developers in the Stack Overflow annual developer survey. Source:* https://survey.stackoverflow.co/2025/work#salary-comp-total

FIGURE 10: Forking as technical debt

Organization size	Number of employees	Average number of private forks	Average number of labour hours per fork per release	Total labour hours spent each release cycle	Total amount spent each release cycle
Small	1 to 249	7	21	147	$7,350
Medium	250 to 4,999	89	56	4,984	$249,200
Large	More than 5,000	136	82	11,152	$557,600

2025 Open Source ROI Survey, Q32 by Q13, Sample size = 236

Action: Audit private forks and invest in upstream contribution
Private fork maintenance is one of the most significant and underappreciated costs of CRA compliance, consuming thousands of engineering hours per release cycle. Organizations should conduct a systematic audit of their private fork inventory, identify components where elimination of the fork or where upstream contribution is feasible, and develop a structured contribution strategy.

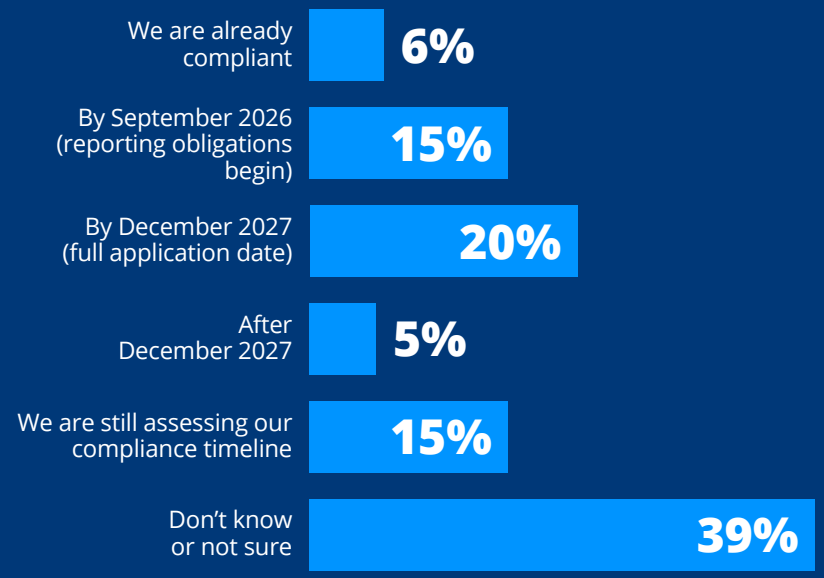
Compliance timelines and pricing impacts

The 2026 survey asked manufacturers directly about their expected compliance timeline and anticipated pricing impacts. The answers reveal both the depth of uncertainty and the likely economic consequences of CRA compliance.

As shown in **FIGURE 11**, only 41% of manufacturers expect to be compliant by December 2027. A further 39% do not know when they will be able to comply. This is a telling indicator of where industry CRA readiness stands, with the deadline for full compliance less than two years away.

FIGURE 11: 39% unsure when they will be able to comply with the CRA

When will your organization fully comply with the CRA? (select one)



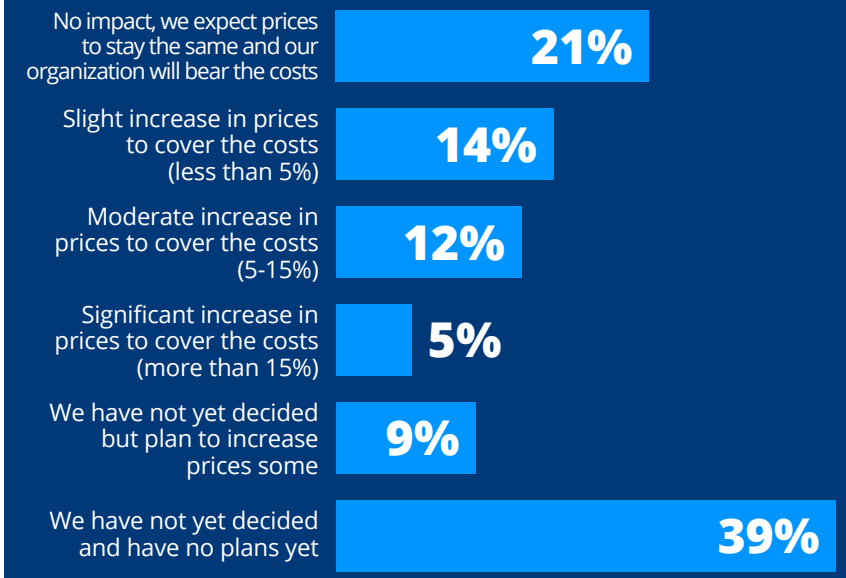
2026 CRA Survey, Q38, Sample size = 194

FIGURE 12 summarizes the implications on cost. 40% of manufacturers indicate they will pass CRA compliance costs on to consumers. The 2025 study found that manufacturers who had assessed their pricing strategy anticipated an average 6% price increase. This year's data shows an average of 4% price increase among those who have decided. The 2026 data also shows slightly less impact on prices, with 21% of respondents

anticipating no impact compared to 14% in 2025. This implies that at least some but likely only a slight or moderate increase will reach consumers in many cases. However, the price differences will likely vary company by company and are prone to changes as the CRA implementation unfolds. We believe organizations that already know about the CRA and pay significant attention to security are likely to have fewer costs. No one, not even the impacted manufacturers, know what the costs will be for manufacturers who are still unaware of the CRA.

FIGURE 12: 40% of organizations will factor in CRA costs into their product prices

How will the costs of implementing CRA compliance factor into your product or solution pricing going forward? (select one)



2026 CRA Survey, Q38, Sample size = 194

For a comparison with 2025 data, please see Appendix A11.

SME vulnerability in light of the CRA

According to the **European Union's publication** on the impact of OSS in the European economy, small and medium-sized enterprises (SMEs) are critical drivers of innovation and competitiveness within the EU ICT sector. A recent **call for evidence** by the European Commission can also provide further references to the importance of SMEs in Europe's IT industry. As the segment that benefits most from the low barriers to entry of open source collaboration, SMEs are also the most at risk from CRA compliance requirements.The 2026 data reveals that SMEs are simultaneously more exposed to CRA obligations (due to their higher relative OSS dependency) and potentially less able to absorb compliance costs (**FIGURE 13**).

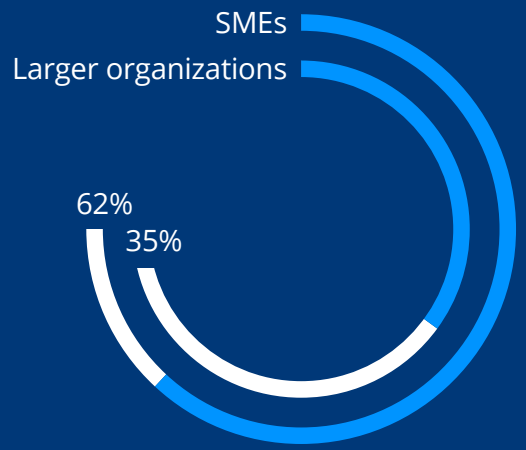
The concentration of SMEs in the high-OSS-dependency bracket is not surprising. This is because smaller organizations are less likely to have the resources to develop proprietary components from scratch. But this dependency means they must manage extensive OSS supply chains with limited security and legal expertise and often no dedicated compliance unit.

European SMEs show unfamiliarity at 51%, which means that every second SME in our survey is unfamiliar or slightly familiar with the CRA. This is important not only for the businesses themselves, but for the broader health of the European digital economy. SMEs are the backbone of the EU's technology ecosystem, accounting for the vast majority of businesses and a substantial share of software innovation and supply chain activity across the continent.

FIGURE 14 shows that SMEs are more likely than larger organizations to pass compliance costs on to consumers, with 47% of SME manufacturers planning some form of price increase compared to 40% overall. Moreover, 11% of surveyed organizations expect significant increases above 15%. At the same time, SMEs bear proportionally higher per-unit

FIGURE 13: SME Vulnerability

% of organizations where more than 75% of their products rely on OSS



SME unfamiliarity with the CRA

55%

European SME unfamiliarity with the CRA

51%

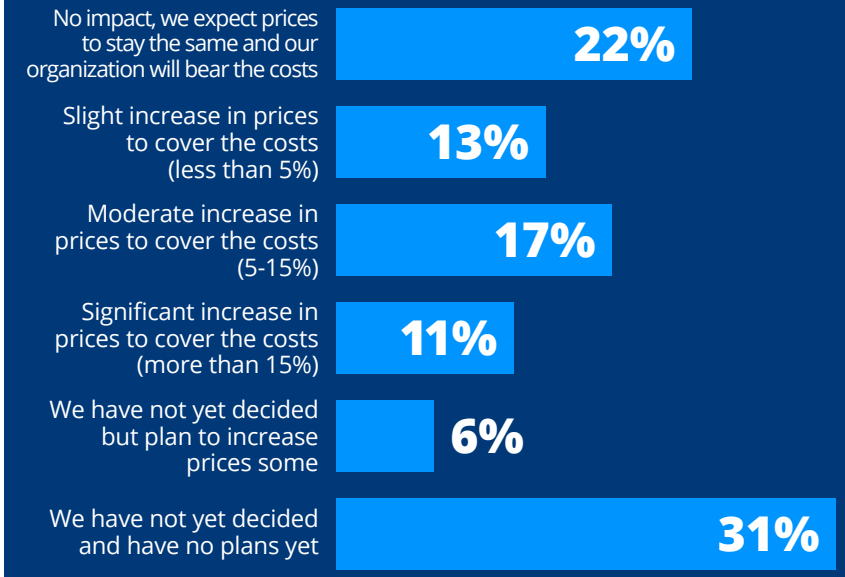
2026 CRA Survey, Q27, Q14 filtered for SMEs and SMEs in Europe, Sample size = 187, 162, 96

For complete data, see Appendix A12-A14.

compliance costs. A large enterprise may distribute the cost of security audits, SBOM tooling, and vulnerability management infrastructure across a large revenue base. However, a smaller software company building IoT products might not be able to. Without targeted SME support mechanisms, CRA compliance may risk becoming a structural barrier to SME participation in the EU market.

FIGURE 14: 47% of SMEs will factor in CRA costs into their product prices

How will the costs of implementing CRA compliance factor into your product or solution pricing going forward? (select one)



2026 CRA Survey, Q38, Sample size = 54 (filtered for SME manufacturers)

Action: Bring SME voices into the CRA conversation

Much of the guidance, tooling, and research shaping CRA implementation has been developed from the perspective of larger organizations with dedicated legal, security, and compliance functions, a lens that may not reflect the realities SMEs face. Actively seeking out and amplifying SME perspectives would produce a more complete picture of what compliance actually looks like at the scale at which most European software businesses operate.

From the experts

HARALD FISCHER
Security Aspect Lead, Balena

balena

We see a critical lack of CRA awareness in the IoT and embedded space. Users struggle to classify products and solutions, define responsibility boundaries and understand which essential cybersecurity requirements they must implement. Furthermore, IoT devices often require seven to ten years of security support. This demands robust operational tools, not just awareness. We agree with the report findings that the industry needs explicit implementation steps, especially regarding the secure use of open source software in regulated products. We actively share our findings and collaborate within the OpenSSF. Facing this regulation together in the open drives the best industry readiness.

Stewards and open source projects

Steward readiness

The CRA defines OSS stewards the following way:

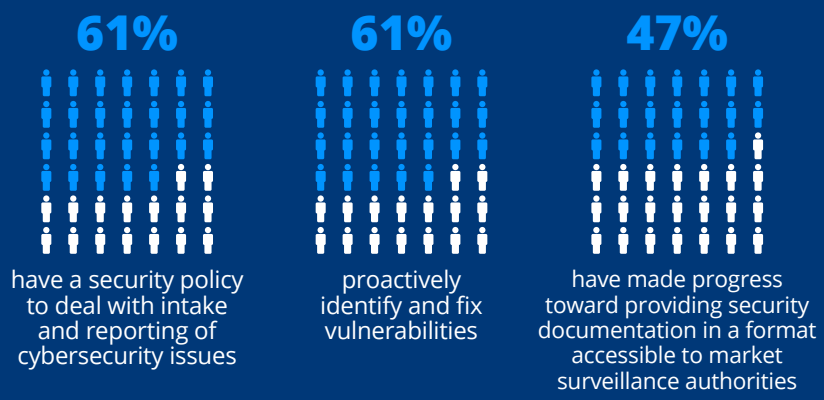
> *'open-source software steward' means a legal person, other than a manufacturer, that has the purpose or objective of systematically providing support on a sustained basis for the development of specific products with digital elements, qualifying as free and open-source software and intended for commercial activities, and that ensures the viability of those products;* (CRA **article 3**).

OSS stewards under the CRA are regulated with a lighter regulatory touch than manufacturers. Stewards must establish cybersecurity policies, notify authorities of actively exploited vulnerabilities, and promote vulnerability information sharing within the community among other requirements. (CRA **article 24**).

FIGURE 15 suggests that steward-organized projects are already on track to meet their legal obligations. The data show an encouraging sign that the open source community is moving in the right direction, even ahead of formal enforcement. This is further evidenced by a Linux Foundation case study report titled **Pathways to Cybersecurity Best Practices in Open Source** examining how three well-established LF-hosted projects are already meeting CRA obligations in practice. Drawing on the experiences of the Yocto Project, Zephyr Project, and the Civil Infrastructure Platform: Industrial Grade Linux, the report offers concrete, tried-and-tested pathways for the broader open source community to consider when preparing for the new regulatory requirements. While challenges remain, the

report's core message is that investment in security tooling, cross-community collaboration, and proactive engagement with emerging threats such as AI-driven risks will be essential for stewards seeking to meet their CRA obligations.

FIGURE 15: Stewards are on track to meet legal obligations



2026 CRA Survey Q41, Q42, Q47, Sample size = 28

For complete data and a comparison with 2025, please consult Appendix A15-A17.

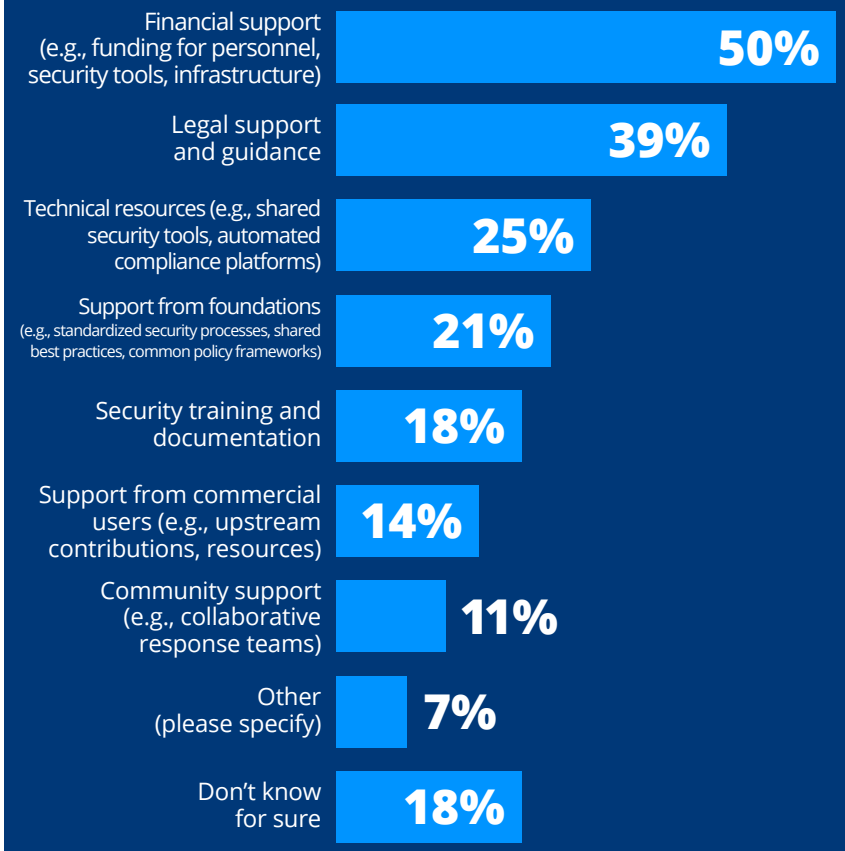
Note on the steward sample: The steward sample (n=28) is small. The results and its comparison to 2025 should be interpreted as indicative, not definitive.

As shown in **FIGURE 16**, the top two needs stated by stewards are financial support and legal guidance, which cannot be met by documentation alone. They require structural investment: foundation-level funding for steward organizations, compliance best practices, and shared security infrastructure that smaller projects can plug into without building from scratch.

Beyond financial support (50%) and legal guidance (39%), a quarter (25%) of stewards also cite the need for technical resources such as shared security tooling and automated compliance platforms, while a further 21% look to foundations for standardized security processes and common policy frameworks. Taken together, these findings paint a picture of a steward community that would appreciate resources to meet the requirements fully, including financial and legal support that could clear uncertainties around steward obligations.

FIGURE 16: What stewards need

What support do your projects most need to meet CRA requirements? (select up to three responses)



2026 CRA survey, Q53, Sample size = 28, Total mentions = 57

Action: Build shared compliance infrastructure for stewards
The OpenSSF OSPS Baseline and the OpenSSF Best Practices Badge provide a starting point for security attestation. Foundations can extend this by offering: (1) legal review services for steward organizations navigating CRA classification; (2) shared SBOM generation tooling that stewards can adopt without standing up their own infrastructure; and (3) model security policies (SECURITY.md templates, CVE triage workflows) aligned to CRA requirements.

Non-commercial OSS perspective

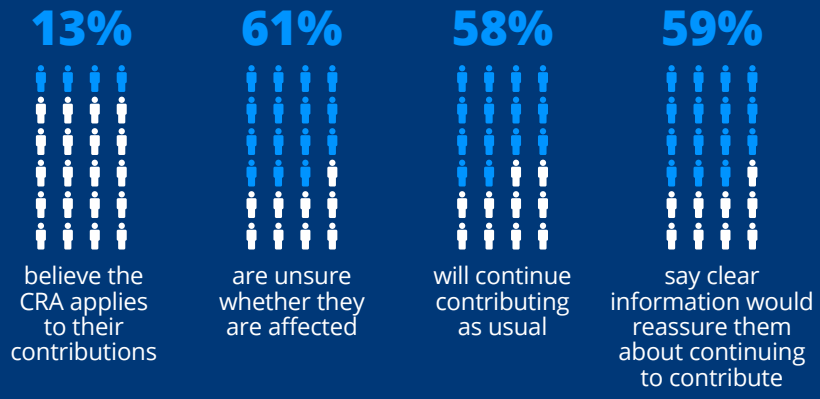
The CRA explicitly excludes non-commercial OSS development from its scope, but among the 109 non-commercial developers surveyed, significant uncertainty persists about whether the regulation applies to them.

The CRA's explicit exemption of non-commercial open source contributors has been one of the regulation's most debated design choices, and the data in **FIGURE 17** help to explain why clarity on this point matters in practice. Consistent with last year's findings, a portion (13%) of non-commercial contributors believe the CRA applies to their contributions and 61% are unsure whether they are affected at all. While 58% say they will continue contributing as usual, a significant share remain hesitant or undecided. Crucially, 59% say that clear information would reassure them about continuing to contribute, pointing to a straightforward and high-impact intervention that has yet to be fully seized. That this need remains as acute in 2026 as it was in 2025 should sharpen the sense of urgency around delivering that clarity before the December 2027 deadline.

After the survey closed, in March 2026, the European Commission published its first **comprehensive draft guidance** on the CRA, which specifically addresses free and open source software. The draft guidance was open for public consultation and, together with the **Commission's FAQ**, is intended to reduce uncertainty, and will likely become a key reference point for both companies and market surveillance authorities once finalized.

The data make clear that what non-commercial contributors need is not more general awareness of the CRA, but specific, practical clarity about how it applies or does not apply to them. As **FIGURE 18** shows, the two most requested resources are clear explanations of how the CRA applies to individuals (70%) and concrete examples of scenarios where the CRA does or does not apply (69%). Educational resources and foundation or regulator guidance follow at 50% and 48% respectively, reinforcing that contributors are actively seeking authoritative, accessible information rather than abstract legal analysis. The **OpenSSF CRA Brief Guide for OSS Developers** is a step in this direction, but the data suggest the guide's scenario library needs to be expanded and more actively promoted. At the time of writing another valuable resource came out, published by OpenSSF and dedicated to maintainers and developers: the **CRA Readiness Guide for Maintainers and Developers**.

FIGURE 17: Contributors are unclear how the CRA impacts them



2026 CRA Survey Q54, Q55, Q56, Sample size = 109

For complete data and a comparison with 2025, please see Appendix A18-A20.

FIGURE 18: Resources for OSS contributors

What would help you better understand the CRA and its impact on your OSS contributions? (select all that apply)

2026 CRA Survey, Q57, Sample size = 109, Total mentions = 271

Security posture and vulnerability trends of open source projects

Beyond the survey data, this report draws on a second source of evidence to give insights into the security posture of 12,863 important open source software projects indexed in the **LFX platform**. Where the survey captures perceptions, intentions, and self-reported practices, the LFX data provides a ground-level view of where open source projects stand on the security measures that the CRA will increasingly demand.

Security posture and readiness varies considerably by project aspect. In **FIGURE 19**, we plot average scores from the OpenSSF Scorecard[2] checks for the sample of top open source projects. The evidence in **FIGURE 19** demonstrates that projects on average excel in some categories and require improvements in others, suggesting considerable scope for improvement in security posture for top open source projects. For example, projects typically do a good job fixing existing vulnerabilities (79%), declaring a license (75%), and keeping the source tree free of binary artifacts (98%). Projects have a more mediocre security posture when it comes to avoiding dangerous workflows (45%), establishing code review protocols (39%), and explicitly defining a security policy (31%). Fewer projects implement some practices such as signing releases (1%), setting proper CI token permissions (5%), or pinned dependencies (6%).

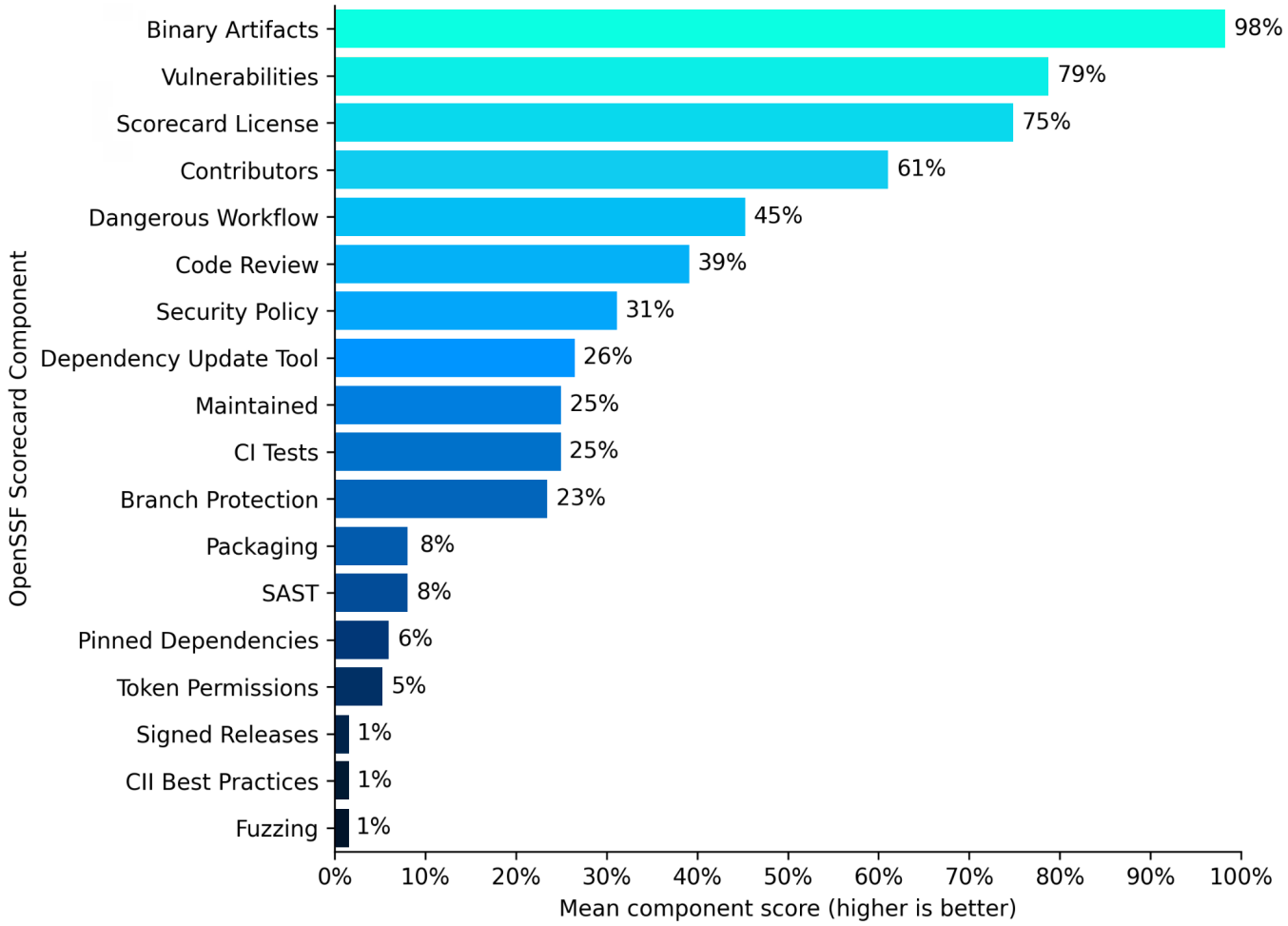
Most important from a CRA compliance perspective are practices which are in serious need of improvement across the ecosystem, such as signing releases and setting proper CI token permissions. The CRA presents an opportunity to incentivize these supply chain integrity controls.

FIGURE 20 shows further analysis of the security data. Organizational diversity is highly correlated with both (1) security posture and (2) economic value of the project. The number of distinct organizations that contribute to a project and the CLOMonitor Security score[3] have a Spearman correlation coefficient of **0.57**, indicating a strong positive relationship between security and organizational diversity. The correlation coefficient between organizational diversity and OpenSSF Best Practices score is **0.40**. Furthermore, organizational diversity is also related to project complexity and replacement cost: the correlation coefficient between a project's organizational diversity and COCOMO valuation is **0.52**.

[2] *The OpenSSF Scorecard is a framework for metrics to measure the extent to which open software components adhere to security best practices.*

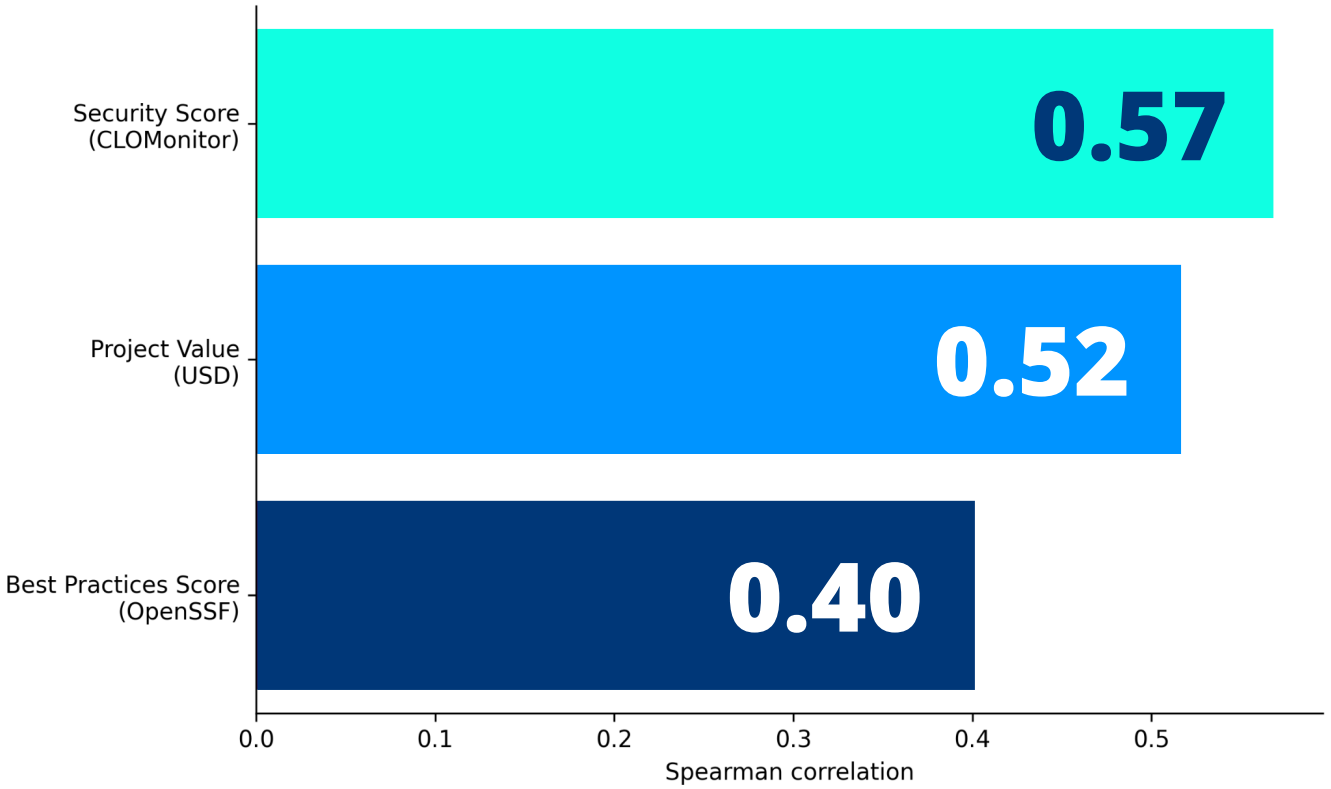
[3] *Developed by the Cloud Native Computing Foundation, CLOMonitor is "a tool that periodically checks open source projects repositories to verify they meet certain project health best practices"*

FIGURE 19: Dimensional breakdown of security posture



LFX curated data based on reports generated between 03/08/2024 and 06/03/2025

FIGURE 20: Number of contributing organizations coincides with both security posture and economic value



LFX curated data based on reports generated between 03/08/2024 and 06/03/2025

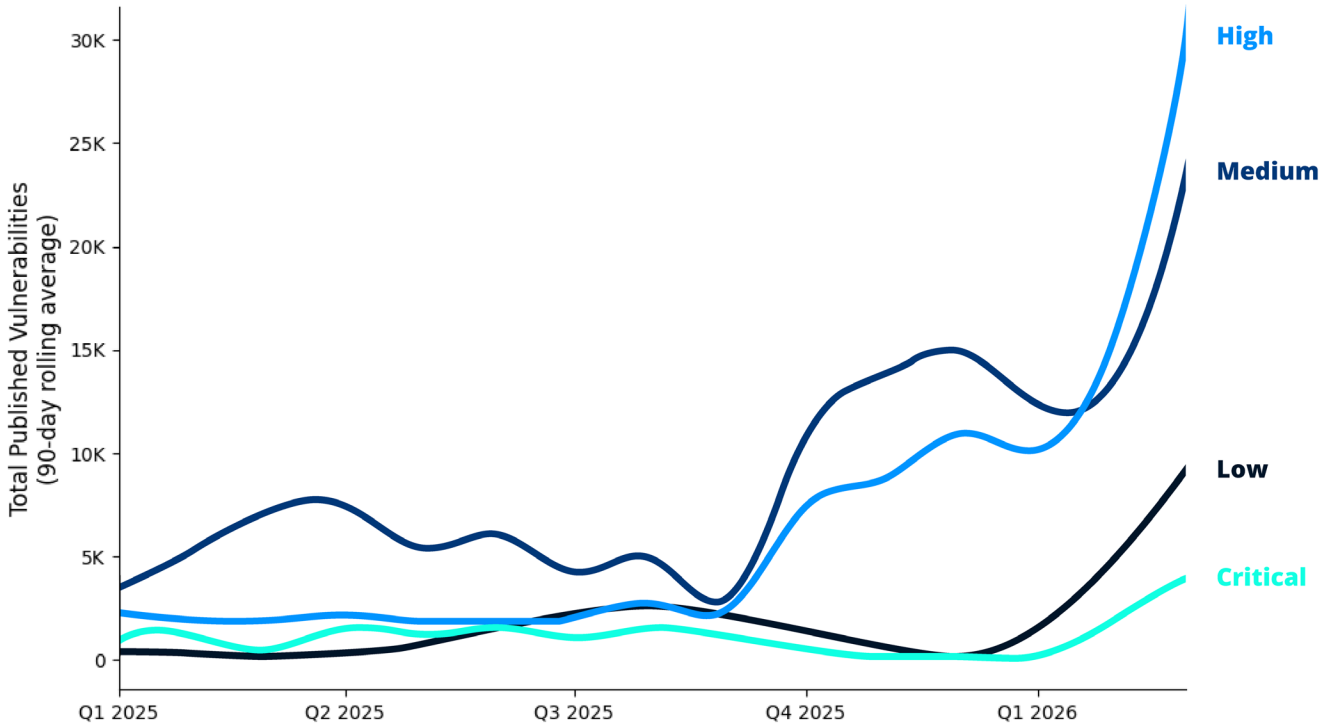
Action: Invest in the open source projects you depend on

The more organizations contribute to a project, the better its security outcomes tend to be. This means that investing in the open source projects in their supply chain is a direct investment in their own compliance posture. The alternative, relying on underfunded and narrowly maintained projects, while expecting them to meet the security standards the CRA demands without aid from the organizations that use it, is a risk that will only become harder to ignore as the December 2027 deadline approaches.

FIGURE 21 gives a view into the prevalence of security vulnerabilities ecosystem-wide, plotting the 90 day rolling average of newly published vulnerabilities across 14,204 open source software projects indexed on LFX. There has been an explosion in CVE discoveries over the past year, with nearly exponential growth since the beginning of 2025. Q1 2026 saw a staggering 394% year-over-year increase in published CVEs, up by 101,489 total vulnerabilities across all repositories. Most alarming was the growth in high-severity (+811%) and critical-severity (+136%) threats.

This was also confirmed in the **NIST update**, which found that submissions during the first three months of 2026 are nearly one-third higher than the same period last year. However, this surge warrants careful interpretation. A significant portion likely reflects the rapid proliferation of AI-based automated vulnerability scanning tools and broader project indexing coverage, meaning more vulnerabilities are being discovered and reported rather than purely introduced. Regulatory pressure from the CRA have also likely accelerated internal audits of dependency trees, surfacing latent issues

FIGURE 21: Exponential growth in discovered vulnerabilities



LFX curated data

that previously went unlogged. Further analysis is needed to distinguish which automatically detected vulnerabilities pose actual high risks from those that are false positives.

The distinction of true risk and false alarms is particularly significant in the context of the CRA, which mandates that manufacturers address reported vulnerabilities. If a large proportion of automatically detected vulnerabilities turn out to be false positives, manufacturers risk being overwhelmed by remediation obligations for issues that do not pose meaningful threats. It could also divert resources away from vulnerabilities that genuinely require attention.

For the CRA, the findings in this section carry a pointed implication. The regulation places obligations on manufacturers to exercise due diligence over their software supply chains, but the security quality of the open source components they depend on is itself a function of how well-supported those projects are. Projects sustained by a single organization or a narrow contributor base (often maintained by only one person) are more likely to exhibit weaker security postures.

The number of vulnerabilities discovered are also growing. While AI-based automated scanning likely accounts for much of this increase, the trend is that manufacturers are substantially exposed to the risks. Upstream investment and engagement will be the practical lever for raising the security baseline of the components that CRA compliance ultimately depends on. Organizations can choose to create and maintain their own components and component forks, at substantial cost, or work with other organizations to better support the OSS they depend on, which is less expensive long-term for organizations, is better for OSS, and is better for society.

From the experts

EDDIE KNIGHT
Founder, Revanite

REVANITE

Much like the official CRA guidance, open source solutions are constantly evolving— and anyone can lend their voice to help accelerate the ecosystem. Even as a small team, Revanite has contributed several high-impact elements to the OpenSSF: We launched the OSPS Baseline, crafted an automated scanner to evaluate compliance with it, and created the Gemara project to streamline end-to-end machine-readable compliance workflows. Now, we're joining some of the biggest players in the industry to create the emerging "CRA Baseline for Manufacturers," where we strongly encourage other SME firms to come shape the future with us!

Conclusion

The 2026 CRA Awareness and Readiness Report documents a moment of genuine challenge, but also of genuine possibility. The regulation is in force, the deadlines are known, and the open source community has the tools, talent, and collaborative instincts to meet what is being asked of it. What remains is for manufacturers to act, and to choose the more sustainable path while there is still time to do so.

The awareness gap is real, but it need not be permanent. The materials and initiatives that exist, such as the **LFEL1001 training course**, the OpenSSF OSPS Baseline, and foundation-hosted technical projects, are already rated highly by those who find them. The challenge is about awareness of them rather than quality. Redirecting outreach toward the developer spaces where practitioners actually learn, such as conferences, documentation, social media, and podcasts, could be a clear path to closing the gap before the December 2027 deadline.

The economics of CRA compliance, though daunting on the surface, point toward a model that is better for everyone. The significant costs of private fork maintenance, when made visible, make the case for upstream contribution more compellingly than any policy argument could. Organizations that invest in the open source projects they depend on do not just reduce their compliance burden but also strengthen the shared infrastructure that the entire software ecosystem runs on. The CRA, in this sense, may incentivize an ecosystem where upstream contribution is the default, financially rational choice.

The security analysis and vulnerability trends of over 12,000 open source projects tells a similar story. CVEs detected across the ecosystem rose 394% year-over-year in Q1 2026, a surge driven in part by better AI-based automated detection but one that nonetheless reflects a substantial vulnerability burden. Against that backdrop, organizational diversity emerges as a strong predictor of security posture, meaning that broadening participation in open source projects is itself a compliance strategy. Every organization that engages upstream, funds a maintainer, or contributes a security fix is directly improving the reliability of the supply chain the CRA is designed to protect.

For SMEs, stewards, and non-commercial developers, the road ahead is more navigable than it may appear. Targeted support mechanisms, shared compliance infrastructure, and clear scenario-based guidance can meaningfully reduce the burden on those least equipped to bear it alone. The OpenSSF's **EU Cyber Resilience Act (CRA) page** links to many OpenSSF resources such as the **Linux Foundation CRA Stewards Playbook**, **Linux Foundation Leadership CRA Stewards One Pager**, **CRA Readiness Guide for Maintainers and Developers** and the **Cyber Resilience Act (CRA) Brief Guide for Open Source Software (OSS) Developers**. The European Commission's March 2026 **draft guidance** on free and open source software, as well as the **FAQ document** published in December 2025, are a promising step in this direction, and its finalization will give a large and currently uncertain segment of the community the clarity it has been waiting for.

The 2027 deadline is a forcing function, but it points toward something worth building: software supply chains that are more secure, and more sustainably supported than those that exist today.

Resources

European Commission Resources

- **Full regulatory text of the CRA**
- **Draft guidance on free and open source software**
- **Cyber Resilience Act implementation - FAQ document**

OpenSSF and Linux Foundation Resources

- **EU Cyber Resilience Act (CRA) page**
- **Linux Foundation CRA Stewards Playbook**
- **Linux Foundation Leadership CRA Stewards One Pager**
- **CRA Readiness Guide for Maintainers and Developers**
- **Cyber Resilience Act (CRA) Brief Guide for Open Source Software (OSS) Developers**

Global Cyber Policy Working Group Resources:

- **Global Cyber Policy WG GitHub**
- **#wg-globalcyberpolicy on Slack**
- **Global Cyber Policy WG Mailing List**
- **CRA Readiness+Awareness SIG Mailing List**
- **CRA Tooling+Process+Formats SIG Mailing List**
- **CRA Spec Standardization SIG Mailing List**

Vulnerabilities Reporting & Guidance:

- Guidelines on reporting **vulnerabilities specific to LF projects and foundations**.
- **List of Linux Foundation projects**
- Linux kernel security vulnerabilities should be reported to security@kernel.org as described in the **Linux kernel security bugs page**.
- Report vulnerabilities specific to Linux Foundation infrastructure or the main LF website by emailing security@linuxfoundation.org
- **Alert on social engineering takeovers**

Security Best Practices and Tools:

- **Alpha Omega** partners with OSS project maintainers to systematically find and fix new, as-yet-undiscovered vulnerabilities in open source code
- **CNCF fuzzing handbook** describes what fuzzing is and how to apply it
- **OpenSSF Technical Initiatives**, including Best Practices Badge, Scorecard, Sigstore and more
- **System Package Data Exchange (SPDX)** open SBOM standard (ISO/IEC 5692:2021)
- **Post Quantum Cryptography Alliance** for the adoption and advancement of post quantum cryptography

Educational Resources:

Featured Certifications

- **Kubernetes and Cloud Native Security Associate** (KCSA)
- **Certified Kubernetes Security Specialist** (CKS)

Instructor-Led Training Courses

- **Security and the Linux Kernel** (LFD441)
- **Kubernetes Security Fundamentals** (LFS460)
- **Zero Trust Security with SPIFFE and SPIRE** (LFS482)
- **Security Coding Fundamentals** (WSKF601)
- **Understanding Vulnerabilities and Security Threats** (WSKF603)

Hands-On Learning Workshops

- **Securing Coding Fundamentals** (WSKF601)
- **Understanding Vulnerabilities and Security Threats** (WSKF603)

Featured Free Training

- **Developing Secure Software** (LFD121)
- **Developing Secure Software - Japanese version** (LFD121-JP)
- **Securing Your Software Supply Chain with Sigstore** (LFS182)
- **Understanding the OWASP® Top 10 Security Threats** (SKF100)
- **Introduction to DevSecOps for Managers** (LFS180)
- **Introduction to Zero Trust** (LFS183)
- **Cybersecurity Essentials** (A Must-Have for ALL Employees) (LFC108)

Free Express Learning (60–90 minutes)

- **Security Self-Assessments for Open Source Projects** (LFEL1005)
- **Securing Projects with OpenSSF Scorecard** (LFEL1006)
- **Automating Supply Chain Security: SBOMs and Signatures** (LFEL1007)

e-Learning Courses

- **Kubernetes Security Essentials** (LFS260)
- **Mastering Kubernetes Security with Kyverno** (LFS255)
- **Modern Air Gap Software Delivery** (LFS281)
- **Implementing DevSecOps** (LFS262)
- **Mastering Infrastructure Security: Strategies, Tools, and Practices** (SKF200)
- **Cloud Native Fuzzing Fundamentals** (LFS251)
- **Detecting Cloud Runtime Threats with Falco** (LFS254)

Research

- **Unaware and Uncertain: The Stark Realities of Cyber Resilience Act Readiness in Open Source Report** - This survey-based report investigates the awareness and readiness of the open source community to comply with the EU's Cyber Resilience Act.
- **ROI for Open Source Software Contribution** - In this study, LF Research has tackled the question on the benefits of contributing to open source through the analysis of results from a survey and quantitative model on contribution ROI.
- **Pathways to Cybersecurity Best Practices in Open Source** - This case study report from the Linux Foundation investigates the impacts of the Cyber Resilience Act on open source software, including new cybersecurity obligations and the role of manufacturers and stewards.
- **The State of Global Open Source 2025** - As part of the ongoing World of Open Source research series, the 2025 edition investigates how open source is adopted across core technology stacks and how organizations employ security evaluation practices, formal governance structures, and support for open source in production environments.
- **The 2025 State of OSPOs and Open Source Management** - In its 8th year, the 2025 edition explores how OSPOs are rapidly maturing from compliance-focused units into strategic governance hubs, with growing roles in risk management, AI oversight, and open source supply chain security.

Methodology

This study is based on a web survey that Linux Foundation Research and the OpenSSF conducted in January 2026. The survey aimed to examine the potential effects of governmental cybersecurity regulations on the OSS ecosystem. A similar study was conducted in January 2025, the results of the two surveys are comparable for year-over-year analysis. In this section, we present the study methodology and context regarding how we analyzed the data followed by the demographics of the respondents.

We addressed data quality through extensive prescreening, survey screening questions, and data quality checks to ensure that respondents had sufficient professional experience to answer questions accurately themselves or on behalf of the organization they worked for.

We collected survey data from industry-specific companies, IT vendors and service providers, and nonprofit, academic, and government organizations. Respondents spanned many vertical industries and companies of all sizes, and we collected data from several geographies.

The survey comprised 58 questions that addressed screening, respondent demographics, CRA awareness, and CRA role self-identification and had specific sections for manufacturers, OSS stewards and non-commercial OSS developers. For information about access to the survey, its dataset, and survey frequencies, see the survey data access information below.

The target audience included respondents who met the following criteria:

- **Must be familiar with the concept of OSS**
- **Must be able to identify their involvement with OSS**
- **Must be able to identify their employment status**

The survey was fielded in January 2025. A total of 685 respondents completed the awareness section of the survey. The sample size for manufacturers is 194 to 219. For stewards, it is 28, and for non-commercial OSS developers, it is 109. The margin of error for the awareness sample size is + / - 2.8% at a 90% confidence level and + / - 3.4% at a 95% confidence level.

For information about access to the survey, its dataset, and survey frequencies, see the survey data access information below.

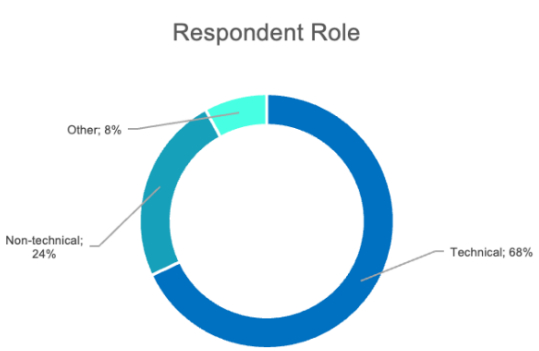
Survey demographics

FIGURE 22 summarizes the most important demographics of the survey. Most respondents are in technical roles. Industry representation was dominated by information technology (48%), followed by financial services (8%) and various other sectors. Organization sizes were well distributed, with 45% representing small organizations (1–249 employees), 26% medium organizations (250–4,999 employees), and 29% large organizations (5,000+ employees). The survey achieved broad geographic representation, with 46% of respondents based in Europe, 26% in the United States/Canada, and 12% in Asia Pacific.

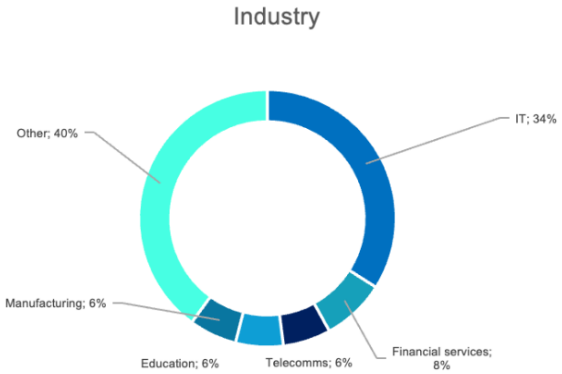
Survey data access

Linux Foundation Research makes each of its empirical project datasets available on Data.World. Included in this dataset are the survey instrument, raw survey data, screening and filtering criteria, and frequency charts for each question in the survey. Linux Foundation Research datasets, including this project, are available at data.world/thelinuxfoundation. Access to Linux Foundation datasets is free but does require you to create a Data.World account.

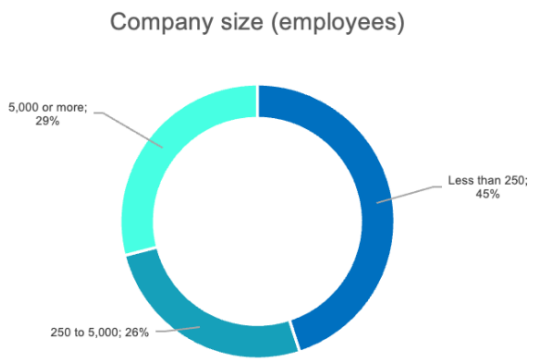
FIGURE 22: Selected demographics from the 2026 CRA survey



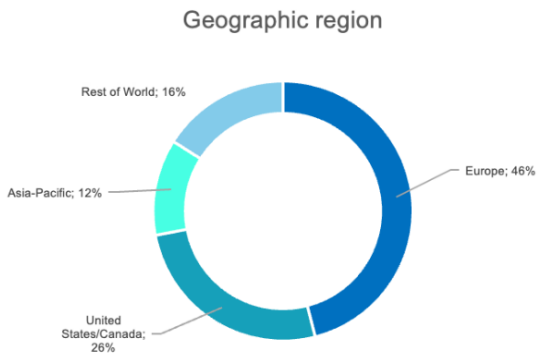
2026 CRA Survey, Q5, Sample Size = 843



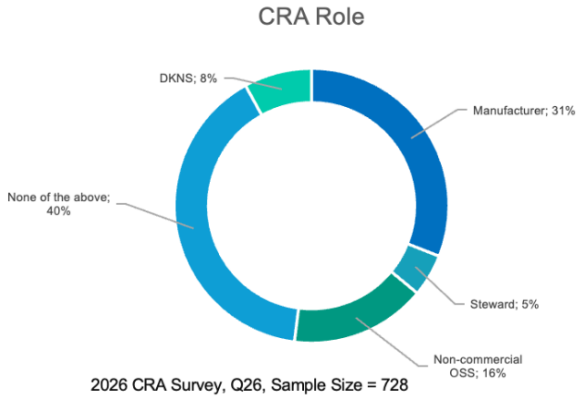
2026 CRA Survey, Q9, Sample Size = 638



2026 CRA Survey, Q10, Sample Size = 625



2026 CRA Survey, Q4, Sample Size = 843



2026 CRA Survey, Q26, Sample Size = 728

2026 CRA Survey, Q26, Sample Size = 728

About the author

ADRIENN LAWSON serves as Director of Quantitative Research at the Linux Foundation, where she leads data-driven initiatives to understand open source ecosystems. With expertise in social data science from the University of Oxford and a background spanning academic and governmental research, she brings methodological rigor to analyzing distributed collaboration networks. At the Linux Foundation, Adrienn leads a team conducting cross-sectional research across industry verticals and geographic regions to provide comprehensive insights into open source dynamics. Her work encompasses empirical investigations into regulatory compliance, the implications of AI, and sustainable funding models. She produces evidence-based recommendations that inform strategic decision-making within the open source community.

Acknowledgments

We thank all the participants of the survey for kindly sharing their insights and experience.

Special thanks to the peer reviewers and Linux Foundation colleagues for their involvement in the various stages of the research process, including Mirko Boehm, Hilary Carter, Mike Dolan, Anna Hermansen, Angelah Liu, Madalin Neag, Christopher (CRob) Robinson, Kate Stewart, David A. Wheeler, and Steve Winslow.

Special thanks to Sam Boysel for his analysis of the LFX security and CVE data and his contributions to the security findings in this report.

LF Research uses generative AI tooling in varying degrees for research-related tasks including aggregating secondary sources, analyzing data, supporting report drafting, copyediting, and translation. All AI-generated content is reviewed and revised as needed.

Thanks to sponsors:

OpenSSF OPEN SOURCE SECURITY FOUNDATION balena ERICSSON REVANITE

Appendix

A1: OVERALL FAMILIARITY LEVELS WITH THE CRA		
How familiar are you with the Cyber Resilience Act (CRA)? (select one)		
	2026	**2025**
Not familiar at all	42%	36%
Slightly familiar	24%	26%
Somewhat familiar	16%	17%
Familiar	9%	12%
Very familiar	6%	5%
Extremely familiar	3%	4%
2026 CRA Survey, Q114, Sample Size = 843; 2025 CRA Survey, Q18, Sample Size = 685		

A2: AWARENESS LEVEL OF THE CRA SEGMENTED BY GEOGRAPHIC REGION				
How familiar are you with the Cyber Resilience Act (CRA)? (select one) segmented by In what country or region do you primarily live? (select one)				
	Total	**Europe**	**USA / Canada**	**Asia-Pacific**
Not familiar at all	40%	36%	52%	31%
Slightly familiar	25%	26%	20%	30%
Somewhat familiar	16%	16%	14%	21%
Familiar	9%	10%	7%	11%
Very familiar	7%	8%	4%	5%
Extremely familiar	3%	4%	3%	2%
2025 CRA Survey, Q14 by Q4, Sample Size = 718				

A3: ORGANIZATIONAL CRA COMPLIANCE

Do you know whether you or your organization must comply with CRA regulations? (select one)

	2026	2025
Yes	59%	58%
No	41%	42%

2026 CRA Survey, Q20, Sample Size = 404; 2025 CRA Survey, Q24, Sample Size = 384

A4: KNOWLEDGE OF CRA IMPLEMENTATION TIMELINE

When will organizations have to fully comply with CRA regulations? (select one)

	2026	2025
2025	5%	11%
2026	12%	6%
2027	34%	28%
2028	3%	4%
Don't know or not sure	46%	51%

2026 CRA Survey, Q18, Sample Size = 404; 2025 CRA Survey, Q22, Sample Size = 384

A5: FAMILIARITY LEVEL WITH THE POTENTIAL PENALTIES OF CRA NON-COMPLIANCE

Are you familiar with the potential penalties if found out of compliance with CRA regulations? (select one)

	2026	2025
Yes	44%	41%
No	56%	59%

2026 CRA Survey, Q21, Sample Size = 404; 2025 CRA Survey, Q25, Sample Size = 384

A6: KNOWLEDGE GAP IN THE DIFFERENCE BETWEEN MANUFACTURERS AND OSS STEWARDS

Are you aware of the distinction between manufacturers and open source software stewards in the CRA? (select one)

	2026	2025
Yes	46%	43%
No	54%	57%

2026 CRA Survey, Q19, Sample Size = 404; 2025 CRA Survey, Q23, Sample Size = 384

A7: LEVEL OF DEPENDENCY TRACKING OF MANUFACTURERS WITH SBOMS

Is your organization producing or preparing to produce Software Bill of Materials (SBOM) or any software used in your products or solutions? (select one)

	2026	2025
Yes, for all products	32%	34%
Yes for some, but not all products	29%	25%
Not for any products, but have plans to	8%	6%
My organization is aware of SBOMs, but not producing them today and has no plan yet	8%	9%
My organization is not aware of SBOMs at all	5%	4%
Don't know or not sure	18%	21%

2026 CRA Survey, Q28, Sample Size = 219; 2025 CRA Survey, Q28, Sample Size = 205

A8: OSS VULNERABILITY RESPONSE STRATEGIES AMONG MANUFACTURERS

If an OSS component in your product has a vulnerability, how do you usually address it? (select one)

	2026	2025
We rely on the OSS project to release a fix	51%	46%
We patch the component internally	23%	20%
We replace the component with a more secure alternative	9%	11%
We use a supported/enterprise version of the component	5%	9%
We notify customers of the issue but do not directly address it	0%	0%
We do not address it	1%	1%
Don't know or not sure	**11%**	**12%**

2026 CRA Survey, Q30, Sample Size = 219; 2025 CRA Survey, Q30, Sample Size = 205

A9: OSS SECURITY VISIBILITY PRACTICES AMONG MANUFACTURERS

Does your organization have visibility into the security posture of the OSS components you use? (select one)

	2026	2025
Yes, we regularly assess security practices of OSS projects	34%	38%
Somewhat, we rely on published updates or community reports	47%	44%
No, we do not monitor the security practices of OSS projects we use	11%	9%
Don't know or not sure	**9%**	**9%**

2026 CRA Survey, Q29, Sample Size = 219; 2025 CRA Survey, Q29, Sample Size = 205

A10: UPSTREAM CYBERSECURITY CONTRIBUTION PLANS UNDER CRA

Does your organization have a plan to contribute cybersecurity fixes upstream once the CRA goes into effect? (select one)

	2026	2025
Yes	22%	22%
No	20%	19%
We already contribute security fixes (patches) back upstream to projects we rely on	19%	16%
Don't know or not sure	39%	44%

2026 CRA Survey, Q34, Sample Size = 194; 2025 CRA Survey, Q34, Sample Size = 180

A11: PRICE IMPACT OF THE CRA

How will the costs of implementing CRA compliance factor into your product or solution pricing going forward? (select one)

	2026	2025
No impact, we expect prices to stay the same and our organization will bear the costs	21%	14%
Slight increase in prices to cover the costs (less than 5%)	14%	13%
Moderate increase in prices to cover the costs (5-15%)	12%	12%
Significant increase in prices to cover the costs (more than 15%)	5%	8%
We have not yet decided but plan to increase prices some	9%	6%
We have not yet decided and have no plans yet	39%	47%

2026 CRA Survey, Q38, Sample Size = 194; 2025 CRA Survey, Q38, Sample Size = 180

A12: OSS RELIANCE ACROSS DIFFERENT ORGANIZATION SIZES

To your knowledge, what percentage of your product(s) relies on open source software? (select one)

	SMEs	Large organizations
Less than 25%	5%	12%
25% to 50%	14%	22%
51% to 75%	14%	16%
More than 75%	62%	35%
Don't know or not sure	5%	14%

2026 CRA Survey, Q27, Sample Size = 187

A13: SME FAMILIARITY LEVELS

How familiar are you with the Cyber Resilience Act (CRA)? (select one) filtered for SMEs

Not familiar at all	30%
Slightly familiar	25%
Somewhat familiar	18%
Familiar	12%
Very familiar	11%
Extremely familiar	5%

2026 CRA Survey, Q14, Sample Size = 162

A14: EUROPEAN SME FAMILIARITY LEVELS

How familiar are you with the Cyber Resilience Act (CRA)? (select one) filtered for SMEs Europe	
Not familiar at all	25%
Slightly familiar	26%
Somewhat familiar	17%
Familiar	13%
Very familiar	14%
Extremely familiar	6%

2026 CRA Survey, Q14, Sample Size = 96

A15: STEWARD READINESS ON PROVIDING CYBERSECURITY POLICY, ARTICLE (24(1))

Do your OSS projects have a security policy to effectively deal with intake and reporting of cybersecurity issues? (select one)		
	2026	**2025**
Yes	61%	74%
No	25%	18%
Don't know or not sure	14%	9%

2026 CRA Survey, Q41, Sample Size = 28; 2025 CRA Survey, Q40, Sample Size = 34

A16: STEWARD READINESS ON FIXING VULNERABILITIES

Do you have a process for identifying and addressing vulnerabilities in your OSS projects? (select one)		
	2026	**2025**
Yes, we proactively identify and fix vulnerabilities	61%	68%
Yes, but we only address vulnerabilities when reported by users	21%	21%
No, we rely on external contributors or users to address issues	11%	6%
Don't know or not sure	7%	6%

2026 CRA Survey, Q42, Sample Size = 28; 2025 CRA Survey, Q41, Sample Size = 34

A17: STEWARD READINESS ON PROVIDING DOCUMENTATION, ARTICLE 24(2)

Can your OSS projects provide documentation about your security measures in a format that market surveillance authorities can easily understand? (select one)

	2026	2025
Yes, documentation ready	7%	9%
Partial documentation available	29%	24%
In progress	11%	12%
No documentation prepared	29%	26%
Don't know or not sure	25%	29%

2026 CRA Survey, Q47, Sample Size = 28, 2025 CRA Survey, Q46, Sample Size = 34

A18: CRA IMPACT ON OSS DEVELOPERS

Do you think the CRA could apply to your open source contributions? (select one)

	2026	2025
No, I don't think it applies to me	27%	24%
Possibly, but I'm not sure	61%	59%
Yes, I believe I may be impacted as a contributor	13%	17%

2026 CRA Survey, Q54, Sample Size = 109; 2025 CRA Survey, Q53, Sample Size = 126

A19: CRA IMPACT ON OSS CONTRIBUTIONS

Does the potential impact of the CRA make you reconsider contributing to OSS? (select one)

	2026	2025
No, I will continue contributing as usual	58%	58%
Somewhat, I am concerned but will continue contributing for now	22%	25%
Yes, I am thinking about reducing or stopping contributions	6%	5%
Don't know or not sure	15%	16%

2026 CRA Survey, Q55, Sample Size = 109; 2025 CRA Survey, Q54, Sample Size = 126

A20: NEED FOR CLEAR INFORMATION		
Would clarification about the CRA help you feel more confident continuing to contribute to OSS? (select one)		
	2026	**2025**
Yes, clear information would reassure me	59%	75%
No, I will still feel uncertain	6%	6%
I'm unsure—it depends on the guidance provided	36%	20%
2026 CRA Survey, Q56, Sample Size = 109; 2025 CRA Survey, Q55, Sample Size = 126		

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

The Open Source Security Foundation (OpenSSF) is a cross-industry organization at the Linux Foundation that brings together the industry's most important open source security initiatives and the individuals and companies that support them. The OpenSSF is committed to collaboration and working both upstream and with existing communities to advance open source security for all. For more information, please visit us at **openssf.org**.

THE LINUX FOUNDATION | Research

Founded in 2021, **Linux Foundation Research** explores the growing scale of open source collaboration, providing insight into emerging technology trends, best practices, and the global impact of open source projects. By leveraging project databases and networks and committing to best practices in quantitative and qualitative methodologies, Linux Foundation Research is creating the go-to library for open source insights for the benefit of organizations worldwide.

To reference this work, please cite as follows: Adrienn Lawson, "2026 CRA Awareness and Readiness Report," foreword by Roman Zhukov, The Linux Foundation, June 2026.

facebook.com/TheLinuxFoundation

x.com/linuxfoundation

linkedin.com/company/TheLinuxFoundation