THE LINUX FOUNDATION Research
OpenSSF OPEN SOURCE SECURITY FOUNDATION
THE LINUX FOUNDATION Europe

Unaware and Uncertain

The Stark Realities of Cyber Resilience Act Readiness in Open Source

Adrienn Lawson, The Linux Foundation
Stephen Hendrick, The Linux Foundation

Foreword by Christopher (CRob) Robinson,
Open Source Security Foundation (OpenSSF)

March 2025

Overall awareness of the CRA is low, with 62% being "not familiar at all" or only "slightly familiar" with the CRA.

51% are uncertain about CRA deadlines; only 28% correctly identified 2027 as the target year for full compliance.

Systems integrators, consultants, & academics do not fit squarely into the roles / responsibilities ascribed by CRA.

Nearly half (46%) of manufacturers **passively rely on upstream OSS projects** for security fixes.

Organizations actively engaging with OSS projects are **twice as likely to assess the security practices** of open source projects compared to passive OSS users.

74% of stewards have security policies in place to intake and report cybersecurity issues.

While only 32% of stewards produce SBOMs, **59% use automated dependency tracking.**

Among developers who undertake **non-commercial OSS development**, 17% incorrectly assume that the CRA applies to their contributions, while 59% are unsure whether they are affected.

CRA is expected to drive a **6% average price increase**, though 53% of manufacturers are still assessing pricing impacts.

Top concerns for manufacturers include **legal complexity and ensuring component safety** from suppliers and OSS projects.

62% of stewards **lack dedicated personnel or resources** for quick incident response times.

Financial support (50%), **legal guidance** (47%), and **technical resources** (44%) are most needed to meet CRA requirements for stewards.

Foreword

The Cyber Resilience Act is one of the most consequential pieces of cybersecurity regulation crafted in recent memory and it will have far-reaching implications for the open source ecosystem for years to come. Almost anyone that lives in, works in, or sells computer-related goods and services within the European Union will need to prepare and act, while other governments around the world are looking at the CRA as a model for their own potential legislative agendas to protect their citizens.

Most of the content and requirements of the legislation are not new to anyone who has been involved in cybersecurity over the years. What is truly unique is how the regulators are working to enforce desired security hygiene and responsible usage and support within hardware and software products, which are often heavily dependent on or sourced from free and open source software. Open source software is the engine of global innovation. The CRA creates a new role within the legal world, the open source software steward, and strongly encourages those downstream to become more involved in supporting the projects and communities they use as part of their commercial offerings.

No matter what someone's role is within the software supply chain (manufacturer, steward, developer, consumer, etc.), there will most likely be changes over the next several years that will need to become compliant with the law when it goes into effect in December 2027. The findings detailed within this report showcase the current state of developers' and organizations' readiness and awareness of the CRA and highlight several key areas we all need to start collaborating on to prepare ourselves, our communities, and our downstreams.

We look forward to exploring this data with you and working together to support our communities and stakeholders as we rise to meet this new challenge.

Christopher (CRob) Robinson, Chief Architect, OpenSSF

Table of Contents

Executive summary

The Cyber Resilience Act (CRA) represents a landmark shift in software security regulation, introducing comprehensive cybersecurity requirements for products with digital elements released in the European Union. This study, based on survey responses from participants across the software industry, reveals critical insights into the current state of CRA awareness and preparedness, with a particular focus on its implications for the OSS ecosystem.

Our research uncovers significant knowledge gaps across the industry: 62% of respondents report low familiarity with the CRA, 51% are uncertain about compliance deadlines, and only 28% correctly identified 2027 as the target year for full compliance. Furthermore, 59% of respondents are unaware of non-compliance penalties, and 56% struggle to understand the crucial distinction between manufacturers and stewards under the regulation, highlighting an urgent need for clearer guidance.

The study identifies three distinct stakeholder groups with varying levels of preparedness. Manufacturers, who bear primary responsibility under the CRA, show concerning gaps in their readiness: only 34% produce comprehensive Software Bills of Materials (SBOMs), and 46% passively rely on upstream projects for security fixes. However, the manufacturers that actively engage with the OSS communities they rely on are demonstrating more mature practices. They have higher rates of security assessment and upstream contributions, providing a model for industry adaptation.

Stewards, while representing a smaller segment (8% of respondents), show encouraging levels of security practice adoption: 74% have security policies in place, and 79% maintain voluntary reporting mechanisms. However, resource constraints remain significant, with 62% lacking dedicated incident response capabilities.

A key finding concerns the regulation's unintended impact on OSS developed outside of the course of commercial activity. Among the developers who undertake non-commercial OSS development, we found that 17% incorrectly assume that the regulation applies to their OSS contributions. An additional 59% are unsure whether they are affected. While the CRA explicitly aims to exclude non-commercial development, this uncertainty could affect OSS developers' contribution patterns.

The research also reveals the economic implications of compliance, with manufacturers who have assessed the impact anticipating an average 6% price increase. However, 53% are still evaluating these costs, indicating significant uncertainty about the regulation's economic impact.

Introduction

The CRA introduces comprehensive cybersecurity requirements for products with digital elements released in the European Union, creating new obligations for suppliers, manufacturers, importers, and distributors of software products. This regulation represents the first major attempt to establish uniform cybersecurity standards across the software and hardware industry, with particular implications for OSS development and distribution.

The timing of this regulation is significant given the current imbalance in the OSS ecosystem. Generally, half of the manufacturers remain passive, indirect, or limited users of OSS despite depending on OSS components for over half their products (Appendix A1).

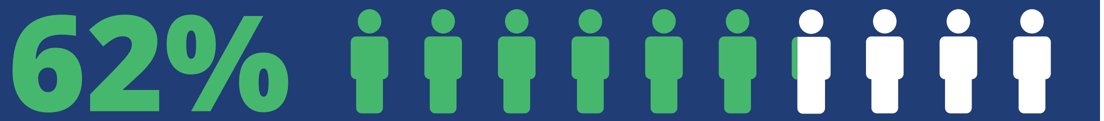
Our research assesses both the current state of CRA awareness and preparation across the software industry, as well as examines how the regulation might address longstanding sustainability challenges in open source. Through detailed survey responses and analysis, we have identified critical gaps in understanding, implementation challenges, and resource constraints that need to be addressed before the CRA takes full effect.

Section 1: CRA awareness: From knowledge gaps to action

1.1 Current state of awareness

Our research uncovered concerning gaps in CRA awareness across all segments of the software industry. Overall awareness levels are notably low, with 62% of respondents reporting that they are either “not familiar at all” or only “slightly familiar” with the regulation. This lack of awareness spans geographic regions, though there are notable variations.

FIGURE 1: Overall CRA awareness level



Overall awareness is low, with 62% being “not familiar at all” or only “slightly familiar” with the CRA

2025 CRA Survey, Q18. Sample size = 685, full chart in Appendix A2

Regional analysis reveals higher levels of unfamiliarity in the U.S./Canada (40%) and Asia Pacific (37%) compared to Europe (29%) (Appendix A3). This geographic disparity is particularly concerning given the global nature of software supply chains and the CRA’s potential impact on any organization providing software to the European market. The observed regional variations in familiarity are not unexpected given that the CRA is primarily a European legislative initiative. However, in light of the global nature of supply chains and the CRA’s extraterritorial reach, organizations outside of Europe will need to elevate their understanding of and compliance with the regulation to maintain market access and avoid potential legal repercussions when their products go to the EU.

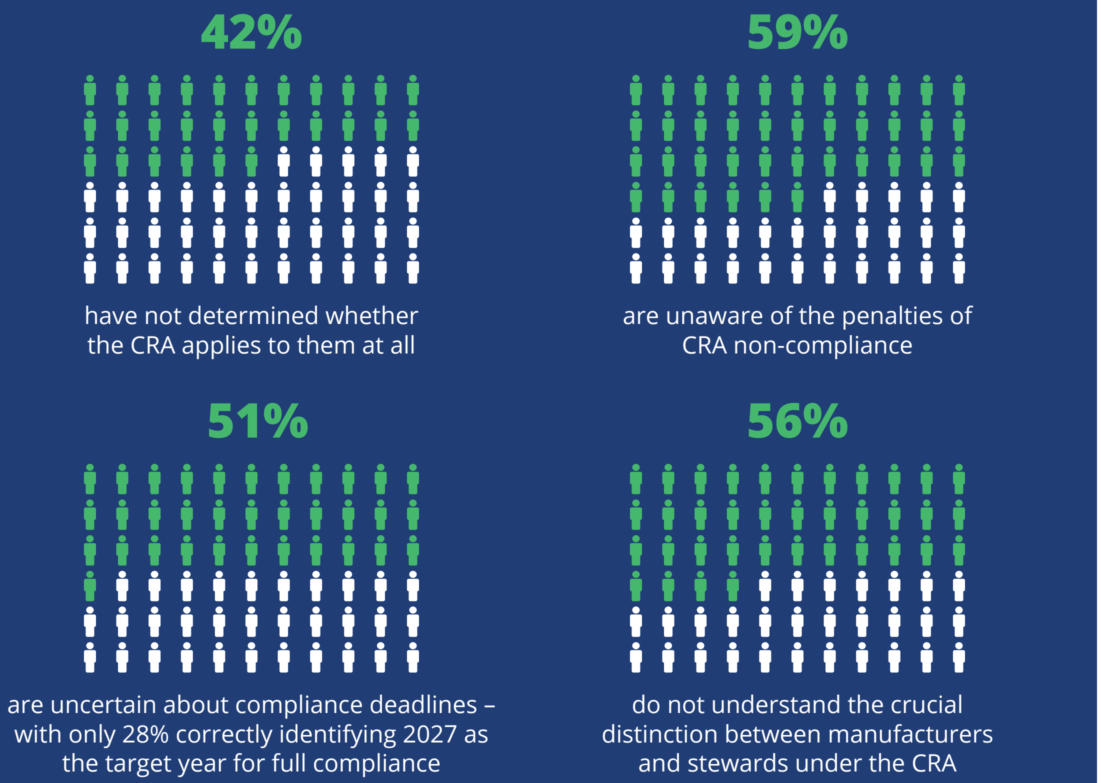
Interestingly, organization size shows limited correlation with awareness levels (Appendix A4). However, we did observe that stewards demonstrate notably higher awareness (42% familiar to extremely familiar) compared to manufacturers (28%), indicating better engagement with regulatory developments among organizations focused on open source maintenance (Appendix A5).

[1] At the time of writing, the following industries and products are CRA exempt: medical devices, motor vehicles, civil aviation products, marine equipment, and military equipment. The European Health Data Space (EDHS) will also amend the CRA to include EHR systems.

1.2 Specific knowledge gaps

Among respondents who reported some familiarity with the CRA, several critical knowledge gaps emerged (Figure 2). We found that 42% of organizations have not yet determined whether the regulation applies to them. This uncertainty could lead to significant compliance challenges as implementation deadlines approach.

FIGURE 2: Specific knowledge gaps: Findings from CRA-aware respondents



have not determined whether the CRA applies to them at all

are unaware of the penalties of CRA non-compliance

are uncertain about compliance deadlines – with only 28% correctly identifying 2027 as the target year for full compliance

do not understand the crucial distinction between manufacturers and stewards under the CRA

2025 CRA Survey, Q24, Q22, Q25. Sample size = 384, full charts in Appendix A6–A9

The survey also revealed that 51% of respondents are uncertain about compliance deadlines, with only 28% correctly identifying 2027 as the target year for full compliance. Furthermore, 59% 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 (Figure 2).

The distinction between manufacturers and stewards under the CRA represents another key area for knowledge development. Currently, 56% of respondents are working to understand these classifications, underscoring the value of creating clear frameworks and guidelines to help organizations accurately determine their roles and corresponding obligations. This knowledge gap becomes particularly significant when examining real-world implementation scenarios. While the CRA's regulatory framework establishes distinct categories for different types of software providers, our research reveals significant challenges in applying these classifications to real-world organizational structures.

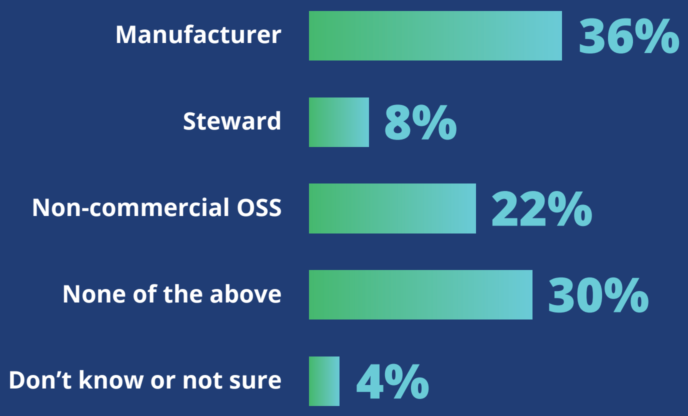
Section 2: CRA classifications meet real-world complexity

The CRA's regulatory framework establishes distinct categories for software providers, primarily distinguishing between manufacturers and OSS stewards. While manufacturers bear full CRA regulatory responsibilities, OSS stewards operate under a lighter regulatory regime — a deliberate approach designed to balance security requirements with the unique contributory nature of OSS development. The CRA also attempts to make a fundamental distinction regarding intent: developers who create software without commercial intent should fall outside the regulation's scope.

While the categories might appear clear in theory, the practical implementation of these distinctions proves considerably more complex, particularly in cases where organizations and individuals fulfill multiple roles within the open source ecosystem.

FIGURE 3: CRA role self-identification

Regarding your use and contribution to OSS, which of the following perspectives are you most qualified to represent in completing this survey? (select one)



Manufacturer = "I work for a company that manufactures or develops products with digital elements (e.g., software, IoT devices, connected products) for commercial use in the European Union (EU) market and these products incorporate OSS components."

Steward = "I work for (or am sponsored by) an organization that develops OSS projects or components intended for commercial use in the EU market."

Non-commercial OSS = "I voluntarily develop OSS projects (independently or as part of a team or community) with no expectation of profit and not intended for commercial use."

2025 CRA Survey, Q23. Sample size = 384

As shown in Figure 3, survey results indicate that two-thirds of respondents (66%) were able to classify themselves within CRA roles, with 36% identifying as working for manufacturers, 8% as working for stewards, and 22% as non-commercial developers. The limited number of respondents identifying as stewards in our survey aligns with expected ecosystem demographics. While individual maintainers are numerous in the open source ecosystem, organizations formally taking on steward responsibilities under the CRA's definition represent a more select group, typically comprising open source foundations and dedicated maintainer organizations that support critical projects.

Among the remaining one-third of respondents who selected "None of the above" or "Don't know or not sure," many are IT professionals working in organizations that do not clearly align with CRA categories, such as system integrators, consultants, and academics (48%) (Appendix A31). The IT industry encompasses a wide range of actors beyond traditional software producers. Organizations may simultaneously act as system integrators, managed service providers, consultancies, and value-added resellers while also engaging in custom software development for clients. Academic institutions contribute through research, tool development, and open source projects while not primarily targeting commercial markets.

Further complexity emerges within manufacturer organizations themselves, where open source projects may exist as distinct entities with their own governance and maintenance models. Large technology companies often host and maintain significant OSS projects alongside their commercial offerings, creating nested relationships between manufacturer and steward roles.

Section 3: Manufacturers and their OSS dependencies

While the CRA creates extensive obligations for manufacturers across their software development practices, our analysis focuses specifically on their relationship with open source dependencies. This reflects our study's primary aim of understanding the implications for the open source ecosystem. The relationship between manufacturers and their open source components is particularly critical as the CRA introduces new requirements for security assessment and maintenance of software dependencies. Our findings examine current patterns of manufacturer engagement with open source projects — from security posture evaluation to upstream contributions — and highlight examples of effective collaborative practices. Understanding these dynamics is crucial for developing approaches that improve security while supporting the sustainability of the open source ecosystem.

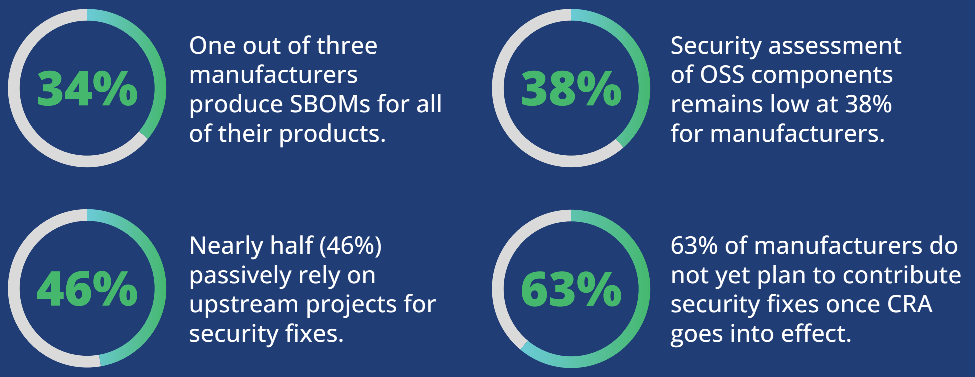
3.1 Current interaction patterns

Our analysis of manufacturer practices reveals significant gaps in preparation for CRA compliance, as shown in Figure 4. Only 34% of manufacturers currently produce SBOMs for all of their products, indicating limited visibility into their software supply chains, despite the CRA's dependency tracking requirements. This gap represents a significant challenge given the regulation's emphasis on supply chain transparency, reporting, and security management.

We also found that nearly half (46%) of manufacturers passively rely on upstream projects for security fixes. This approach may prove insufficient under the CRA's strict vulnerability response timelines, unless resources are allocated to the upstream projects. The survey also revealed that only 38% of manufacturers regularly assess the security practices of their OSS components, falling short of the risk management and documentation mandates outlined in the regulation (Figure 4).

Looking toward future contributions, 44% of manufacturers remain uncertain about their plans for upstream contributions, while 19% have already decided against increasing their engagement (Figure 5). This hesitation suggests many organizations have not yet fully grasped the CRA's implied requirement for the long-time viability of open source components used in their products, potentially creating challenges for long-term compliance.

FIGURE 4: Current interaction patterns between manufacturers and their OSS components in use



One out of three manufacturers produce SBOMs for all of their products.

Security assessment of OSS components remains low at 38% for manufacturers.

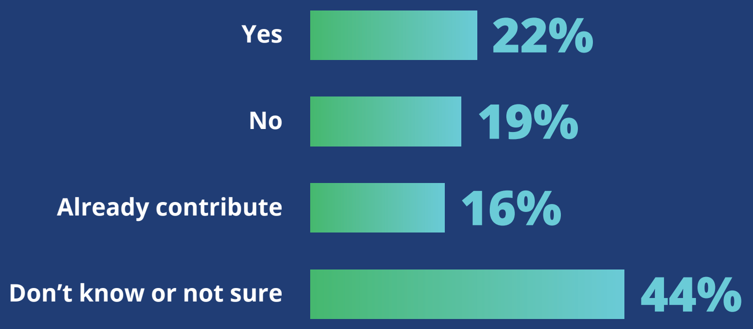
Nearly half (46%) passively rely on upstream projects for security fixes.

63% of manufacturers do not yet plan to contribute security fixes once CRA goes into effect.

2025 CRA Survey, Q28, Q30, Q29, Q34. Sample size = 180–205, full charts in Appendix A10–A13w

FIGURE 5: Upstream cybersecurity contribution plans under CRA

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



2025 CRA Survey, Q34. Sample size = 180

It is important to mention that the CRA places responsibility for security maintenance squarely on manufacturers who integrate open source components into their products. The regulation does not impose obligations on 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. 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.

3.2 Highly engaged organizations as examples of collaborative security

Manufacturers, who actively engage with their OSS dependencies, demonstrate how deep integration with open source communities through active contribution and maintenance benefits both the manufacturer and the broader ecosystem. In contrast, less engaged organizations in our analysis represent manufacturers who remain indirect (relying on third parties to manage OSS components), limited, or passive users of OSS. More engaged organizations demonstrate better preparedness for CRA requirements, as summarized in Figure 6.

FIGURE 6: Highly engaged manufacturers as good examples of collaborative security

High engagers on average have 69% OSS reliance compared to 47% for low engagers

High engagers are twice as likely to assess the security practices of open source projects compared to low engagers

High engagers are more likely to produce SBOMs across all of their products

1 in 3 high engagers (33%) contribute cybersecurity fixes upstream, while only 4% of low engagers do so

2025 CRA Survey, Q27, Q28, Q29, Q34 segmented by Q32. Sample size = 173, full charts in Appendix A14–A17

Further, more engaged manufacturers show an average of 69% OSS reliance compared to 47% for low engagers, indicating deeper integration, even though low engagers demonstrate substantial dependency on open source components for nearly half of their products.

Our research shows that active manufacturers are more likely to produce comprehensive SBOMs across their product lines and are twice as likely to assess the security practices of open source projects compared to more passive consumers. Furthermore, these organizations show significantly higher rates of upstream contributions (Figure 6). They demonstrate that comprehensive open source engagement is not just an aspirational goal but an achievable reality — their existing practices provide a proven model for organizations looking to strengthen their open source security and compliance posture.

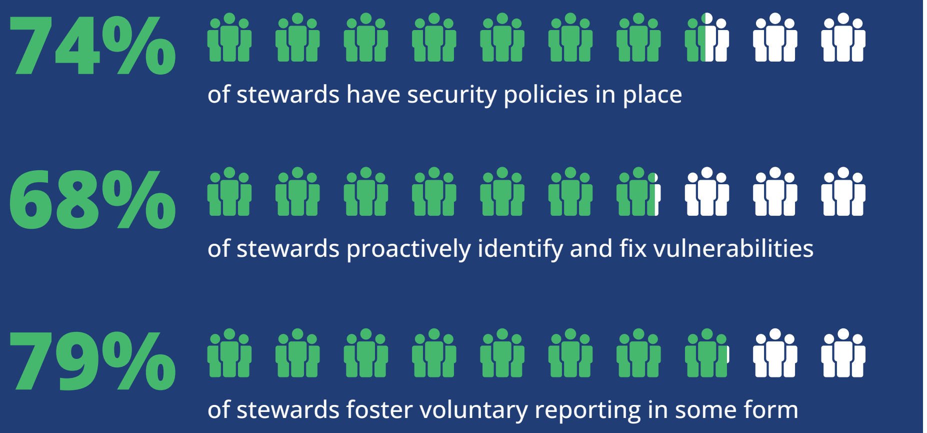
Section 4: Steward CRA readiness

Under the CRA, stewards represent a distinct category encompassing organizations that support OSS intended for commercial use, including certain foundations and entities that develop OSS in a business context, whether for-profit or not. The regulation applies a lighter touch to stewards, focusing on a few key obligations: establishing documented cybersecurity policies, notifying authorities of actively exploited vulnerabilities, and promoting vulnerability information sharing within the open source community. Our assessment of steward readiness, while based on a limited sample of 34 respondents, reflects the relatively small number of organizations that have formally structured themselves around open source support and maintenance. This specialized group, which reported contributions to a total of 325 projects in our survey, provides crucial insights, though the CRA's implementation may influence how many organizations ultimately adopt formal steward roles.

4.1: Existing OSS security practices lay the foundation for CRA compliance

The survey reveals that many organizations classified as stewards under the CRA have already implemented key security practices aligned with the regulation's requirements (Figure 7). Approximately 74% of stewards report having security policies in place, while 68% indicate they proactively identify and fix vulnerabilities. Additionally, 79% of stewards have established some form of voluntary reporting mechanism (such as dedicated security reporting channels), demonstrating a foundation for the transparent security practices the CRA mandates.

FIGURE 7: Existing steward security practice


74% of stewards have security policies in place

68% of stewards proactively identify and fix vulnerabilities

79% of stewards foster voluntary reporting in some form

2025 CRA Survey, Q40, Q41, Q45. Sample size = 34, full charts in Appendix A18–A20

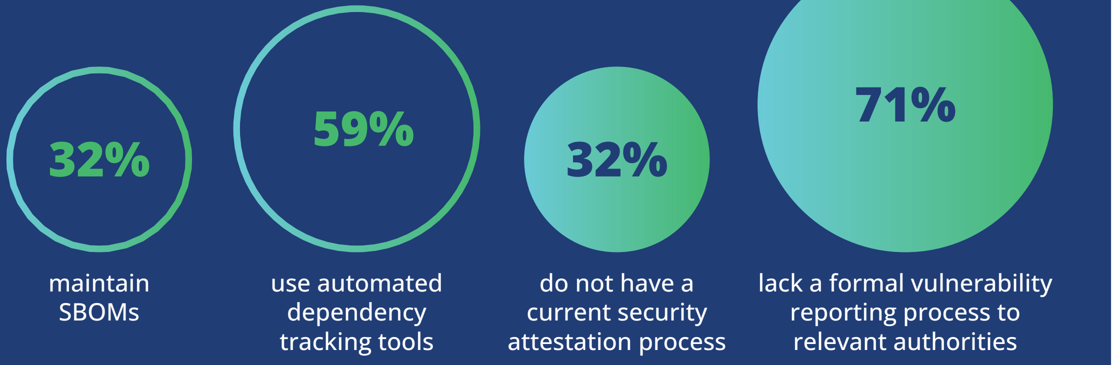
These existing practices provide strong building blocks for CRA compliance. While some standardization and refinement of these mechanisms may be necessary to fully align with the regulation's requirements, these fundamental security practices appear to be largely in place across the steward community.

4.2 Areas for improvement

Despite these positive indicators, some gaps remain in steward preparedness that could enhance the security of the broader software ecosystem. Only 32% of stewards currently maintain comprehensive SBOMs, although 59% use automated dependency tracking tools (Figure 8). While these tools provide a foundation for dependency management, standardized SBOMs would offer additional benefits. For example, they enable system component and license transparency across projects, facilitate automated vulnerability tracking, and provide manufacturers with clear documentation of their supply chain dependencies.

There are also notable limitations in documentation for manufacturer contributions and user communication processes, suggesting a need for standardization in these areas. The survey found that 32% of stewards lack any formal security attestation process, while 71% have not yet established formal vulnerability reporting procedures aligned with CRA requirements (Figure 8). However, these gaps primarily relate to specific CRA documentation requirements rather than fundamental security practices, suggesting they could be addressed through straightforward procedural updates.

FIGURE 8: Areas of improvement for OSS stewards



2025 CRA Survey, Q43, Q49, Q47. Sample size = 34, full charts in Appendix A21–A23

Furthermore, most stewards report minimal readiness for providing documentation to market surveillance authorities, with only 9% indicating they are fully prepared for this aspect of compliance (Appendix A24). This low percentage is unsurprising given that these requirements are specific to the CRA's regulatory framework and will be further detailed in implementing acts by EU authorities. As these requirements become clearer, stewards should be able to adapt their existing security documentation processes to meet compliance needs.

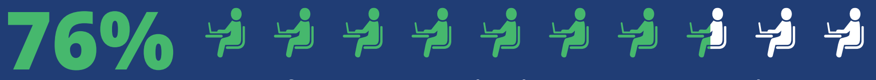
Section 5: Impact on non-commercial OSS development

In this section, we explore the impact of the CRA on open source development that falls outside the scope of commercial activities. It is important to note that the CRA focuses on activities rather than developers themselves. While our survey necessarily collected responses from individuals, our questions aimed to understand the activities they undertake, since the CRA regulates development activities rather than individual developers.

Our study identified which OSS developers this would affect by asking participants to select the perspective they were most qualified to represent in this survey. These developers reported that they voluntarily develop OSS projects with no expectation of profit and no intention for commercial use, as shown in Figure 5.

Survey results show widespread uncertainty about how the CRA will affect OSS developed outside of commercial contexts. We found that 17% of developers incorrectly assume that the regulation applies to their OSS contributions. An additional 59% are unsure whether they are affected (Figure 10). This could mean that three out of four developers may incorrectly assume that the CRA applies to their OSS contributions (Figure 9).

FIGURE 9: Uncertainty around whether CRA applies to OSS contributions



3 out of 4 open source developers may incorrectly assume that the CRA applies to their OSS contributions

2025 CRA Survey, Q53. Sample size = 126, full chart in Appendix A25

FIGURE 10: The CRA's impact on developers who contribute code outside the scope of commercial activity

17% believe CRA applies to their OSS contributions and an additional 59% are unsure whether they are affected

Primary concerns focus on liability for vulnerabilities and confusion about what counts as commercial work

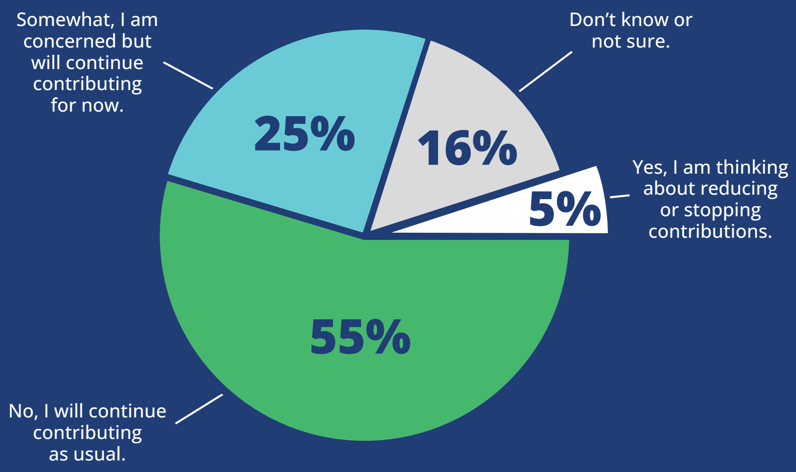
75% indicate clear guidance would help increase confidence

Developers seek clear explanations about how CRA applies to individuals and example scenarios

2025 CRA Survey, Q53, Q57, Q55, Q56. Sample size = 126, full charts in Appendix A25–A28

FIGURE 11: The CRA's potential impact on open source contributions

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



2025 CRA Survey, Q54. Sample size = 126

This uncertainty has led to varying responses, with 5% of developers considering reducing their contributions and 25% expressing concern while continuing their current level of involvement (Figure 11). These findings point to an unintended consequence of the regulation. While the CRA explicitly aimed to exclude open source development that falls outside of commercial activities from its regulatory scope, the lack of clarity is creating hesitation among developers who should be able to continue their work unencumbered.

Encouragingly, 75% of non-commercial developers indicated that clearer guidance would help increase their confidence in continuing their open source work (Figure 10). This strong desire for clarification suggests that targeted communication from regulatory authorities could effectively address current uncertainties. Clear, accessible guidance focusing on how the CRA affects individuals versus organizations, alongside practical examples of when the regulation does and does not apply, would be particularly valuable. These real-world scenarios could help non-commercial developers better understand their position relative to the regulation and confidently continue their valuable contributions to the open source ecosystem.

Section 6: Challenges and next steps

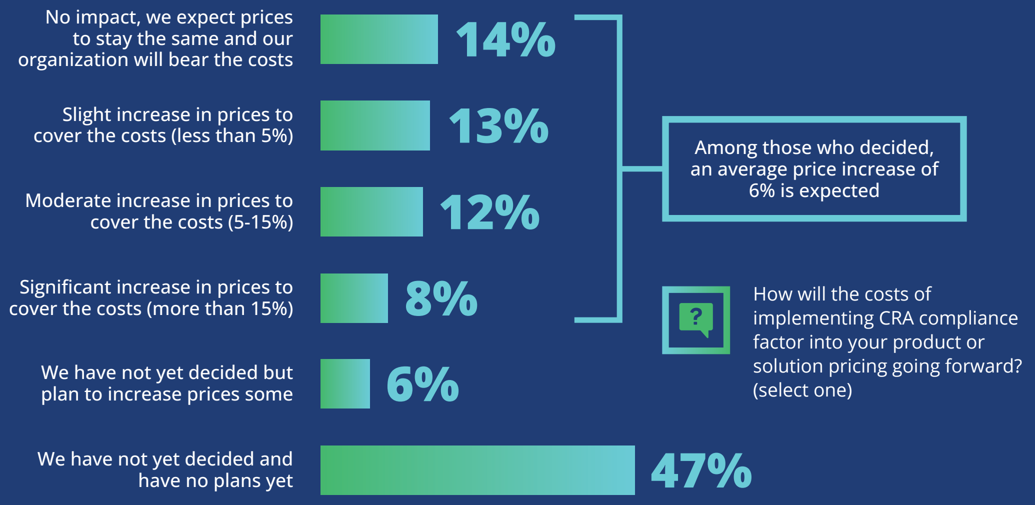
6.1 Strategic implications for manufacturers

Manufacturers face several critical challenges in preparing for CRA compliance. The survey identified legal complexity and compliance understanding as primary concerns, followed by challenges in ensuring component safety from suppliers and OSS projects (Appendix A29). The implications of this latter challenge are significant: manufacturers may need to fundamentally reshape their approach to open source component management, moving from passive consumption to active engagement with their dependencies.

Organizations also expressed significant concern about documentation requirements and the cost implications of the CRA. While 53% of manufacturers have not yet determined how these additional requirements will affect their pricing strategies, those who have made preliminary assessments anticipate an average price increase of 6% (Figure 12). This suggests that the market is still evaluating the full economic impact of CRA compliance, with potential implications for software pricing and accessibility.

When asked about immediate priorities for CRA preparation (Figure 13), manufacturers identified three key areas of focus. The top priority, which 41% of respondents cited, is conducting a comprehensive gap analysis to assess the current practices against CRA requirements. Following closely, 38% of manufacturers prioritize the adoption of essential tooling for SBOM generation, vulnerability scanning, and compliance tracking. The third priority, mentioned by 35% of respondents, focuses on embedding cybersecurity considerations into development lifecycles and supply chain workflows.

FIGURE 12: CRA's potential impact on product pricing



Among those who decided, an average price increase of 6% is expected

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

2025 CRA Survey, Q38. Sample size = 173

6.2 Resource constraints of stewards

The survey revealed significant resource constraints among open source projects that could create challenges in the CRA ecosystem (Figure 14). While 32% of steward organizations report having dedicated resources for incident response, the majority face resource limitations: 56% lack dedicated personnel or funding, and 6% explicitly state they cannot respond quickly to security incidents. These findings become particularly significant when juxtaposed with the manufacturer expectations that we discussed above, where 46% of manufacturers currently rely passively on upstream projects for security fixes.

The situation becomes even more complex when considering that this data only reflects steward-supported projects, which typically have more structured support. Independent, community-based projects that manufacturers also rely on likely have even less capacity for rapid security response. The survey reveals clear priorities for addressing these resource gaps: 50% of projects identify financial support for personnel, security tools, and infrastructure as their primary need, followed by legal support and guidance (47%) and technical resources such as shared security tools and automated compliance platforms (44%) (Appendix A31).

This misalignment between manufacturer expectations and the realities of open source project resources suggests that manufacturers may need to take more active roles in vulnerability remediation, either by developing internal capabilities or contributing resources and fixes back to the projects they depend upon.

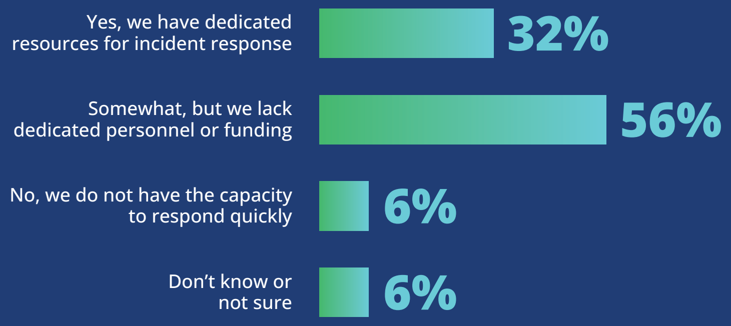
FIGURE 13: Top three priorities to address CRA requirements for manufacturers

1. **Gap Analysis:** Conduct an assessment of current practices against CRA requirements (41%)
2. **Tools and Automation:** Adopt tools for SBOM generation, vulnerability scanning, and compliance tracking (38%)
3. **Process Integration:** Embed cybersecurity into the development lifecycle and supply chain workflows (35%)

2025 CRA Survey, Q37. Sample size = 180, valid cases = 180, total mentions = 386, full chart in Appendix A30

FIGURE 14: Open source software projects' capacity to quickly respond to incidents

Do your projects have the capacity to respond quickly to security incidents or compliance issues in your OSS project? (select one)



2025 CRA Survey, Q50, Sample size = 34

Section 7: Recommendations

Our survey findings reveal both challenges and opportunities in preparing for CRA implementation. Drawing on responses from manufacturers, stewards, and OSS developers, we recommend the following strategic initiatives to strengthen security practices while preserving the open source ecosystem's collaborative nature.

First, manufacturers must transform from passive OSS consumers into active contributors, as they bear primary responsibility under the CRA for security maintenance of their dependencies. While 46% currently rely on upstream fixes, we believe the regulation requires a more proactive approach. This transformation requires manufacturers to develop internal security capabilities, establish formal contribution processes, and allocate resources to support the projects they depend upon.

Second, stewards—particularly those with established security practices and resources—can help scale and standardize security practices across the OSS ecosystem. Organizations such as the Open Source Security Foundation (OpenSSF) demonstrate how stewards can provide value through initiatives such as the OpenSSF's Best Practices Badge program, OpenSSF Scorecard, SBOM generation tools and standards, and vulnerability disclosure frameworks.

Third, regulatory authorities and industry bodies—while ensuring security objectives are met—should prioritize developing clear CRA guidance that explicitly protects OSS development, including those falling outside commercial activities. With 76% of OSS developers uncertain about the CRA's impact, clear examples and scenarios distinguishing regulated from non-regulated activities are essential. This guidance should include simplified compliance documentation and explicit scope limitations for non-commercial projects.

Finally, foundations and similar organizations can serve as strategic bridges between commercial and community interests. With 26% of projects specifically requesting foundation support for standardized security processes, these organizations are well-positioned to facilitate manufacturer-community collaboration, provide shared infrastructure and tools, and support standardization efforts that benefit all stakeholders. We note that the OpenSSF is developing a course (LFEL1001) to help software developers better understand the CRA.

While the primary responsibility for CRA compliance rests with manufacturers, these complementary initiatives from better-resourced stakeholders can help build a more resilient and secure open source ecosystem.

Resources

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

- Empirically driven, security-specific insights from LF Research

Methodology

This study is based on a web survey that Linux Foundation Research and the OpenSSF conducted in January 2025. The survey aimed to examine the potential effects of governmental cybersecurity regulations on the OSS ecosystem. In this section, we present the study methodology and context regarding how we analyzed the data followed by the demographics of the respondents.

From a research perspective, it was important to eliminate any perception of sample bias and ensure high data quality. We handled the elimination of sample bias by sourcing our usable sample from Linux Foundation subscribers, members, partner communities, and social media. 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 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**

Survey development by Linux Foundation Research occurred in December 2024 and January 2025, and 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 180 to 205. For stewards, it is 34, and for OSS developers, it is 126. The margin of error for the awareness sample size is + / - 3.2% at a 90% confidence level and + / - 3.8% at a 95% confidence level.

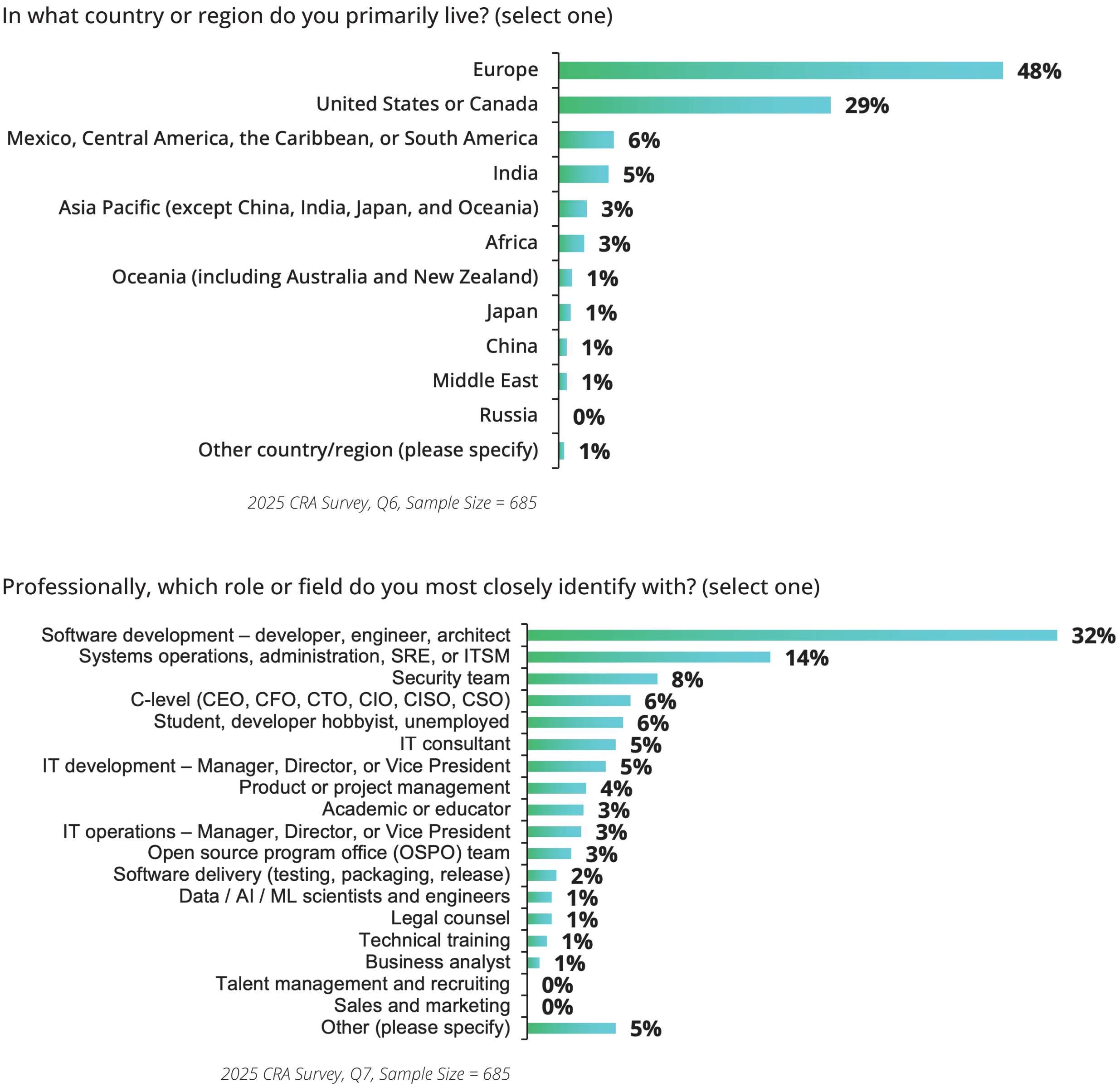
Survey demographics

As shown in Figure 15, the survey achieved broad geographic representation, with 48% of respondents based in Europe, 29% in the United States/Canada, and 10% in Asia Pacific. Most respondents are in technical roles.

As shown in Figure 16, industry representation was dominated by information technology (38%), followed by financial services (8%) and various other sectors. Organization sizes were well distributed, with 41% representing small organizations (1–249 employees), 29% medium organizations (250–4,999 employees), and 28% large organizations (5,000+ employees).

Demographics I

FIGURE 15: Selected demographics from the 2025 CRA Survey



In what country or region do you primarily live? (select one)

2025 CRA Survey, Q6, Sample Size = 685

Professionally, which role or field do you most closely identify with? (select one)

2025 CRA Survey, Q7, Sample Size = 685

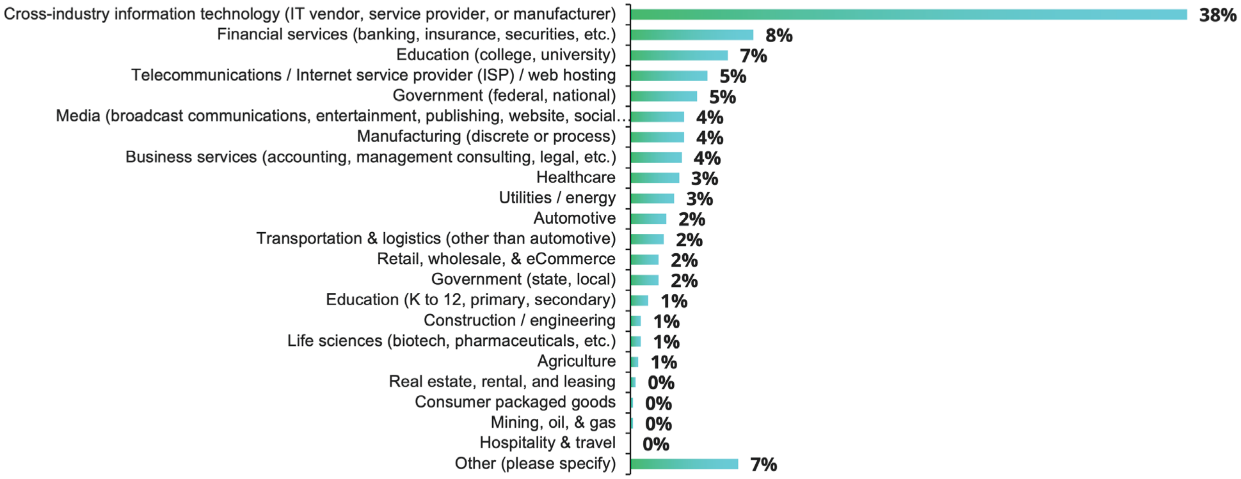
Survey data access

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.

Demographics II

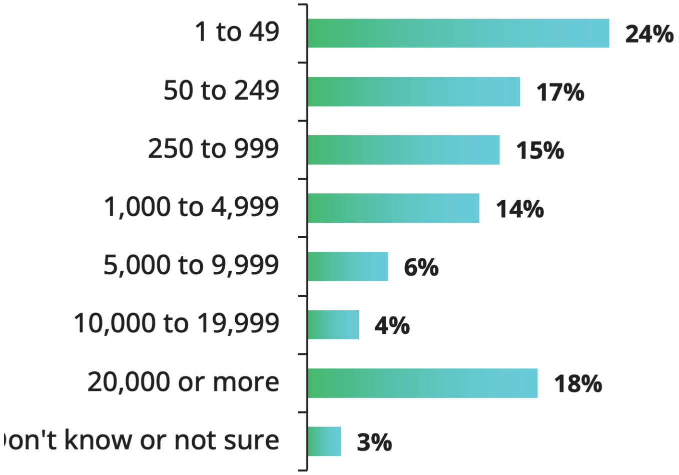
FIGURE 16: Selected demographics from the 2025 CRA Survey

Which of the following best describes your organization's primary industry? (select one)



2025 CRA Survey, Q14, Sample Size = 570

Please estimate how many total employees are in the company or entity you work for. (select one)



2025 CRA Survey, Q15, Sample Size = 570

About the authors

ADRIENN LAWSON is a data analyst at the Linux Foundation. Adrienn obtained a master’s degree in social data science from the University of Oxford. She is responsible for survey development, analysis, and report writing. Adrienn has previously conducted research at the University of Oxford, the Budapest Institute for Policy Analysis, and the U.K.’s Office for National Statistics. She has a strong fascination with the collective power of open source collaboration within geographically dispersed communities. Additionally, she is most interested in researching trends and solutions for challenges related to OSS funding and sustainability and supporting developers in their pursuit of responsible technological advancement.

STEPHEN HENDRICK is the vice president of research at the Linux Foundation, where he is the principal investigator on a variety of research projects core to the Linux Foundation’s understanding of how OSS is an engine of innovation for producers and consumers of IT. Steve specializes in primary research techniques developed over 30 years as a software industry analyst. He is a subject-matter expert in application development and deployment topics, including DevOps, application management, and decision analytics. Steve brings experience in a variety of quantitative and qualitative research techniques that enable deep insight into market dynamics and has pioneered research across many application development and deployment domains. He has authored over 1,000 publications and provided market guidance through syndicated research and custom consulting to the world’s leading software vendors and high-profile start-ups.

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, Elizabeth Bushard, Hilary Carter, Sally Cooper, Mia Chaszeyka, Mike Dolan, Anna Hermansen, Christian (fukami) Horchert, Angelah Liu, Todd Moore, Christina Oliviero, David A. Wheeler, and Christopher (CRob) Robinson.

Appendix

A1: MAPPING PRODUCT DEPENDENCIES AGAINST OSS ENGAGEMENT PATTERNS

To your knowledge, what percentage of your product(s) relies on open source software? (select one) segmented by which of the following best describes your organization's engagement with the OSS projects you rely on? (select one)

OSS contribution level	Average % of OSS reliance
Total	**61%**
Very active: We maintain or regularly contribute code to key projects we depend on.	74%
Moderately active: We occasionally contribute code, report bugs, or improve documentation.	67%
Limited engagement: We mainly report issues and participate in discussions.	50%
Indirect: We rely on commercial suppliers/vendors to engage with the upstream projects	54%
Passive: We use the software but don't actively contribute back.	54%

2025 CRA Survey, Q27 by Q32, Sample Size = 183

A2: OVERALL FAMILIARITY LEVELS WITH THE CRA

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

Not familiar at all	36%
Slightly familiar	26%
Somewhat familiar	17%
Familiar	12%
Very familiar	5%
Extremely familiar	4%

2025 CRA Survey, Q18, Sample Size = 685

A3: AWARENESS LEVEL OF THE CRA SEGMENTED BY GEOGRAPHIC REGION

How familiar are you with the Cybersecurity Resilience Act (CRA)? (select one) segmented by In what country or region do you primarily live? (select one)

	Total	Europe	US/Canada	Asia Pacific
Not familiar at all	**34%**	29%	40%	37%
Slightly familiar	**27%**	27%	26%	27%
Somewhat familiar	**17%**	18%	14%	17%
Familiar	**13%**	14%	10%	14%
Very familiar	**5%**	5%	7%	1%
Extremely familiar	**5%**	6%	2%	4%

2025 CRA Survey, Q18 by Q6, Sample Size = 615

A4: AWARENESS LEVEL OF THE CRA SEGMENTED BY COMPANY SIZE

How familiar are you with the Cybersecurity Resilience Act (CRA)? (select one) segmented by Company size

	Total	Small (1 to 249 employees)	Medium (250 to 4,999 employees)	Large (5000 or more employees)
Not familiar at all	**33%**	32%	36%	32%
Slightly familiar	**25%**	21%	30%	27%
Somewhat familiar	**18%**	20%	15%	18%
Familiar	**13%**	16%	12%	9%
Very familiar	**6%**	6%	2%	10%
Extremely familiar	**5%**	6%	4%	4%

2025 CRA Survey, Q18 by Q15, Sample Size = 555

A5: AWARENESS LEVEL OF THE CRA SEGMENTED BY CRA PERSONA

How familiar are you with the Cybersecurity Resilience Act (CRA)? (select one) segmented by CRA persona

	Total	Manufacturer	Steward	Non-commercial OSS
Not familiar at all	**30%**	30%	20%	34%
Slightly familiar	**25%**	23%	13%	33%
Somewhat familiar	**19%**	21%	24%	14%
Familiar	**15%**	15%	24%	13%
Very familiar	**6%**	9%	7%	2%
Extremely familiar	**5%**	4%	11%	4%

2025 CRA Survey, Q18 by Q26, Sample Size = 389

A6: CRA COMPLIANCE: DO ORGANIZATIONS KNOW IF THEY'RE AFFECTED?

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

Yes	58%
No	42%

2025 CRA Survey, Q24, Sample Size = 384

A7: CRA IMPLEMENTATION TIMELINE: LIMITED UNDERSTANDING OF KEY DATES

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

2025	11%
2026	6%
2027	28%
2028	4%
Don't know or not sure	51%

2025 CRA Survey, Q22, Sample Size = 384

A8: 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)	
Yes	41%
No	59%

2025 CRA Survey, Q25, Sample Size = 384

A9: 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)	
Yes	43%
No	57%

2025 CRA Survey, Q23, Sample Size = 384

A10: LEVEL OF DEPENDENCY TRACKING OF MANUFACTURERS WITH SBOMS

Is your organization producing or preparing to produce Software Bill of Materials (SBOM) for any software used in your products or solutions? (select one)	
Yes, for all products.	34%
Yes for some, but not all products.	25%
Not for any products, but have plans to.	6%
My organization is aware of SBOMs, but not producing them today and has no plan yet.	9%
My organization is not aware of SBOMs at all.	4%
Don't know or not sure	21%

2025 CRA Survey, Q28, Sample Size = 205

A11: OSS VULNERABILITY RESPONSE STRATEGIES AMONG MANUFACTURERS

If an OSS component in your product has a vulnerability, how do you usually address it? (select one)	
We rely on the OSS project to release a fix.	46%
We patch the component internally.	20%
We replace the component with a more secure alternative.	11%
We use a supported/enterprise version of the component.	9%
We notify customers of the issue but do not directly address it.	0%
We do not address it.	1%
Don't know or not sure	12%

2025 CRA Survey, Q30, Sample Size = 205

A12: OSS SECURITY VISIBILITY PRACTICES AMONG MANUFACTURERS

Does your organization have visibility into the security posture of the OSS components you use? (select one)	
Yes, we regularly assess security practices of OSS projects.	38%
Somewhat, we rely on published updates or community reports.	44%
No, we do not monitor the security practices of OSS projects we use.	9%
Don't know or not sure	9%

2025 CRA Survey, Q29, Sample Size = 205

A13: 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)	
Yes	22%
No	19%
We already contribute security fixes (patches) back upstream to projects we rely on.	16%
Don't know or not sure	44%

2025 CRA Survey, Q29, Sample Size = 205

A14: PERCENTAGE OF OSS RELIANCE SEGMENTED BY OSS CONTRIBUTION LEVEL

To your knowledge, what percentage of your product(s) relies on open source software? (select one) segmented by OSS engagement level

	Total	High Engager	Low Engager
Less than 25%	**13%**	5%	21%
25% to 50%	**21%**	18%	23%
51% to 75%	**20%**	17%	22%
More than 75%	**41%**	58%	26%
Don't know or not sure	**5%**	1%	9%
Average		69%	47%

2025 CRA Survey, Q27 by Q32, Sample Size = 193

A15: SBOM PRODUCTION SEGMENTED BY OSS CONTRIBUTION LEVEL

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

	High Engager	Low Engager
Yes, for all products.	43%	26%
Yes for some, but not all products.	27%	25%
Not for any products, but have plans to.	8%	5%
My organization is aware of SBOMs, but not producing them today and has no plan yet.	8%	12%
My organization is not aware of SBOMs at all.	0%	9%
Don't know or not sure	14%	24%

2025 CRA Survey, Q28 by Q32, Sample Size = 193

A16: OSS SECURITY VISIBILITY SEGMENTED BY OSS CONTRIBUTION LEVEL

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

	Total	High Engager	Low Engager
Yes, we regularly assess security practices of OSS projects.	**38%**	51%	26%
Somewhat, we rely on published updates or community reports.	**46%**	36%	55%
No, we do not monitor the security practices of OSS projects we use.	**9%**	7%	12%
Don't know or not sure	**7%**	7%	7%

2025 CRA Survey, Q34 by Q32, Sample Size = 173

A17: PLANS TO CONTRIBUTE CYBERSECURITY FIXES UPSTREAM SEGMENTED BY OSS CONTRIBUTION LEVEL

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

	Total	High Engager	Low Engager
Yes	**21%**	27%	16%
No	**20%**	10%	28%
We already contribute security fixes (patches) back upstream to projects we rely on.	**16%**	30%	4%
Don't know or not sure	**43%**	33%	51%

2025 CRA Survey, Q29 by Q32, Sample Size = 193

A18: 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)

Yes	74%
No	18%
Don't know or not sure	9%

2025 CRA Survey, Q40, Sample Size = 34

A19: STEWARD READINESS ON FIXING VULNERABILITIES

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

2025 CRA Survey, Q41, Sample Size = 34

A20: STEWARD READINESS ON FOSTERING VOLUNTARY REPORTING, ARTICLE 24(1)

How do your projects encourage voluntary reporting of vulnerabilities? (select all that apply)	
We provide dedicated security reporting channels (e.g., security@ email, private vulnerability reporting)	65%
We share advisories about resolved security issues with the community	56%
We maintain a security policy (e.g., SECURITY.md) with reporting guidelines	53%
We have clear processes for handling confidential security reports	50%
We provide templates or guidelines for security reports	24%
We don't have specific measures in place yet	12%
Other (please specify)	9%
Don't know or not sure	9%

2025 CRA Survey, Q45, Sample Size = 34, Valid Cases = 34, Total Mentions = 94

A21: TRACKING DEPENDENCIES IN STEWARD ORGANIZATIONS

How do you track dependencies in your projects? (select all that apply)	
We use automated dependency tracking tools	59%
We maintain SBOMs	32%
We manually maintain a list of dependencies	26%
We track security-critical dependencies separately	15%
We don't currently track dependencies systematically	9%
Don't know or not sure	12%

2025 CRA Survey, Q43, Sample Size = 34, Valid Cases = 34, Total Mentions = 52

A22: STEWARD READINESS IN VOLUNTARY SECURITY ATTESTATIONS (ARTICLE 25)

What does your process for security attestations include? (select all that apply)	
We use automated security scoring tools	21%
We self-attest our security practices through published documentation	18%
We undergo regular third-party security audits	18%
We verify security claims through community review process	18%
We participate in formal security certification programs (e.g., OpenSSF Best Practices Badge)	15%
We maintain compliance with specific security standards	12%
We document our security practices in a standardized format	9%
Our foundation/project has a centralized vulnerability management team that handles this for all of our projects	9%
We don't currently have a security attestation process	32%
Other (please specify)	6%
Don't know or not sure	12%

2025 CRA Survey, Q49, Sample Size = 34, Valid Cases = 34, Total Mentions = 57

A23: STEWARD READINESS IN REPORTING KNOWN ACTIVELY EXPLOITED VULNERABILITIES/NOTIFYING SEVERE INCIDENTS (ARTICLE 24(3))

How does your OSS project(s) report known/actively exploited vulnerabilities? (select one)	
We have an established process for reporting to relevant authorities	29%
We know who to report to but no formal process	18%
We're unsure about reporting requirements/processes	35%
No reporting mechanism in place	18%

2025 CRA Survey, Q47, Sample Size = 34

A24: STEWARD READINESS TO COOPERATE WITH MARKET SURVEILLANCE/PROVIDE 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)	
Yes, documentation ready	9%
Partial documentation available	24%
In progress	12%
No documentation prepared	26%
Don't know or not sure	29%

2025 CRA Survey, Q46, Sample Size = 34

A25: CRA IMPACT ON OSS DEVELOPERS

Do you think the CRA could apply to your open source contributions? (select one)	
No, I don't think it applies to me.	24%
Possibly, but I'm not sure.	59%
Yes, I believe I may be impacted as a contributor.	17%

2025 CRA Survey, Q53, Sample Size = 126

A26: MOST WORRYING SCENARIOS FOR OSS DEVELOPERS	
What specific scenarios worry you about CRA compliance? (select all that apply)	
I might unknowingly introduce vulnerabilities and be held responsible.	54%
Unsure how to distinguish between my hobby contributions and professional work.	44%
Unclear if my project qualifies as commercial when companies use it in their products.	40%
If my OSS project is used at my day job, it might seem like a commercial activity.	33%
Other (please specify)	6%
I'm not worried.	13%
Don't know or not sure	6%
2025 CRA Survey, Q46, Sample Size = 34	

A27: NEED FOR CLEAR INFORMATION	
Would clarification about the CRA help you feel more confident continuing to contribute to OSS? (select one)	
Yes, clear information would reassure me.	75%
No, I will still feel uncertain.	6%
I'm unsure—it depends on the guidance provided.	20%
2025 CRA Survey, Q55, Sample Size = 126	

A28: WAYS TO HELP OSS CONTRIBUTORS

What would help you better understand the CRA and its impact on your OSS contributions? (select all that apply)	
Clear explanations of how CRA applies to individuals.	81%
Examples of scenarios where CRA does or does not apply.	81%
Guidance from open source foundations or regulators.	60%
Educational resources (articles, webinars, workshops).	52%
Other (please specify)	6%
Don't know or not sure	2%

2025 CRA Survey, Q56, Sample Size = 126, Valid Cases = 126, Total Mentions = 356

A29: MAIN CHALLENGES FOR MANUFACTURERS

What challenges do you see in addressing CRA manufacturer requirements? (select all that apply)	
The complexity of the regulations and concern about legal accountability	47%
Ensuring that components from suppliers and OSS projects comply with CRA standards	46%
Providing documentation and proof of compliance with the CRA regulation	42%
The cost of CRA compliance	40%
SBOM generation, updates, and tracking 3rd party dependencies	39%
Aligning CRA requirements with other international regulations	39%
Implementing a secure software development life cycle	36%
Implementing vulnerability management: monitoring, patch management, and vulnerability reporting	32%
Hiring additional cybersecurity staff and addressing training needs	28%
Other (please specify)	2%
No challenges	1%
Don't know or not sure	19%

2025 CRA Survey, Q36, Sample Size = 180, Valid Cases = 180, Total Mentions = 669

A30: TOP PRIORITIES FOR MANUFACTURERS

Which of the following are your organization’s top 3 priorities to address CRA requirements on manufacturers? (select up to three responses)

Gap Analysis: Conduct an assessment of current practices against CRA requirements.	41%
Tools and Automation: Adopt tools for SBOM generation, vulnerability scanning, and compliance tracking.	38%
Process Integration: Embed cybersecurity into the development lifecycle and supply chain workflows.	35%
Workforce Development: Train teams on CRA requirements and best practices.	26%
Collaboration: Work with suppliers, open source projects, and regulators to ensure alignment.	24%
Budget Allocation: Secure funding for the necessary technical and operational upgrades.	18%
Don't know or not sure	32%

2025 CRA Survey, Q37, Sample Size = 180, Valid Cases = 180, Total Mentions = 386

A31: MOST NEEDED RESOURCES FOR STEWARDS

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

Financial support (e.g., funding for personnel, security tools, infrastructure)	50%
Legal support and guidance	47%
Technical resources (e.g., shared security tools, automated compliance platforms)	44%
Support from foundations (e.g., standardized security processes, shared best practices, common policy frameworks)	26%
Support from commercial users (e.g., upstream contributions, resources)	24%
Security training and documentation	18%
Community support (e.g., collaborative response teams)	6%
Other (please specify)	3%
Don't know or not sure	12%

2025 CRA Survey, Q52, Sample Size = 34, Valid Cases = 34, Total Mentions = 78

A32: DISTRIBUTION OF THOSE UNABLE TO IDENTIFY CRA ROLE

Which type of company or entity do you work for? (select one)	
Providing industry-specific products or services	25%
Providing IT products or services (including SIs, IT consultants)	20%
A government (local, county, state, regional, or country)	10%
Non-profit or foundation	4%
An academic organization	8%
Other type of entity (please specify)	6%
Student, developer hobbyist, unemployed, recent graduate, retired (or similar)	27%

2025 CRA Survey, Q12 and Q7, Sample Size = 196

facebook.com/
TheLinuxFoundation

x.com/linuxfoundation

linkedin.com/company/
TheLinuxFoundation

To reference this work, please cite as follows: Adrienn Lawson, Stephen Hendrick, "Unaware and Uncertain: The Stark Realities of Cyber Resilience Act Readiness in Open Source," foreword by Christopher (CRob) Robinson, The Linux Foundation, March 2025.

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

The Open Source Security Foundation (OpenSSF) is a cross-industry initiative by 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 collaborating and working upstream and with existing communities to advance open source security. 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. Through leveraging project databases and networks, and a commitment 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 the world over.