Dialog für Cybersicherheit

Ergebnisbericht

Cybersicherheit in der Gesellschaft – die Rolle des CRA für Open Source

Dialog für Cybersicherheit

Stand: 13.11.2025

CC-BY-SA 4.0

Dialog für Cybersicherheit

Dieser Bericht dokumentiert den Workstream „Cybersicherheit in der Gesellschaft – die Rolle des CRA für Open Source“, der von November 2024 bis November 2025 im Rahmen des Dialogs für Cybersicherheit durchgeführt wurde.

Der Workstream beschäftigte sich mit den Auswirkungen des Cyber Reslience Act (CRA) auf die Open Source Community und hatte dabei insbesondere das Ziel, das Verhältnis der Stakeholder zueinander auszuloten. Es wurde untersucht, wie sich verschiedene Stakeholder zu den im CRA definierten Rollen positionieren. Dabei wurden insbesondere Herausforderungen identifiziert, die sich aus dem Spannungsfeld zwischen den klar abgegrenzten Rollenvorgaben der Regulierung und den dynamischen, oft organischen Strukturen der Open Source Community ergeben.

Ideengeber des Workstreams: Alexander Sander (Free Software Foundation Europe e. V.) und Michael Schuster (BSI)

Beteiligte Mitarbeiter:innen des Workstreams:
Alexander Sander (Free Software Foundation Europe e. V.), Michael Schuster (BSI), Petra Schmidt (CCT - Center for the Cultivation of Technology), Götz Martinek (sodge IT GmbH) Dominik Pataky (CRANIS GmbH), Peter Schoo (privat), Gregor Bransky (Innovationsverbund Öffentliche Gesundheit e. V.)

Der Dialog für Cybersicherheit des Bundesamtes für Sicherheit in der Informationstechnik ist ein partizipativ ausgerichteter gesamtgesellschaftlicher Dialog, um die Vielschichtigkeit der Perspektiven auf das Thema Cybersicherheit möglichst breit und realitätsnah abzubilden und allen Beteiligten einen Austausch bzw. eine Mitwirkung auf Augenhöhe zu ermöglichen.

Der Dialog für Cybersicherheit soll daher ausdrücklich den verschiedenen Meinungen und Ansätzen zur Annäherung an das Thema Cybersicherheit aus Sicht der Zivilgesellschaft Raum und die Möglichkeit zum Austausch geben, ohne dies durch eine engmaschige Steuerung des BSI zu beschränken.

Der vorliegende Bericht wurde von der BSI-Geschäftsstelle und den Workstream-Teilnehmenden eigenständig erarbeitet. Die dort wiedergegebenen Ansichten spiegeln nicht zwangsläufig die Ansicht des BSI bzw. aller Teilnehmenden wider.
Weitere Informationen zum Dialog für Cybersicherheit:
http://www.dialog-cybersicherheit.de

Kontakt Geschäftsstelle: projekt-digitalegesellschaft@bsi.bund.de

Lizenz: Dieser Bericht steht unter der Lizenz Creative Commons CC-BY-SA-Lizenz 4.0 International.

Inhalt

Inhalt 4

Executive Summary 5

1. Einleitung 7

2. Vorgehen 8

2.1. Projektplan 8
2.2. Arbeitspakte im Detail 9
2.2.1. Erstellung der Wissensgrundlage (AP 1 Recherche und AP 5 CRA-Auslegung) ... 9
2.2.2. Vorbereitung und Durchführung der Stakeholderbefragung (AP 2 Stakeholder Ansprache, AP 3 Fragebögen, AP 4 Auswertung) 9
2.2.3. Begleitende Öffentlichkeitsarbeit (AP 6 EU-Begleitung, AP 7 Outreach) 9
2.2.4. Dokumentation und Wissensspeicher 10
3. Ergebnisse 10

3.1. Ergebnisse der Öffentlichkeitsarbeit 10
3.2. Ergebnisse der Stakeholder Befragung 12
3.2.1. Allgemeines 12
3.2.2. Ergebnisse der Herstellerbefragung 12
3.2.3. Ergebnisse der Befragung der Stewards 26
3.2.4. Ergebnisse der Befragung der Maintainer von Open Source Projekten 33
3.2.5. Unterstützungsleistungen 37
4. Fazit 37

5. Anlage: Fragebögen und Auswertung 39

Executive Summary

Mit der Implementierung des Cyber Resilience Act (CRA) wird innerhalb der Europäischen Union (EU) eine horizontale Regulierung für die Cybersicherheit digitaler Produkte etabliert. Bereits im Vorfeld gab es ausgiebige Diskussionen über die Behandlung von Open Source Software (OSS) durch den CRA, welche insbesondere in einigen Ausnahmen innerhalb des CRA für nicht kommerzielle Open Source Softwarehersteller mündete. Hintergrund ist primär der Gedanke, dass dem Ökosystem freier und ohne kommerziellen Zweck geschaffener Open Source Software, nicht die gleichen Compliance-Pflichten wie ihrem profitorientierten Gegenstück zugemutet werden kann.
Da in der Welt der OSS, ein Stück Software selten monolithisch für sich steht, ist die Open Source Community jedoch trotzdem vom CRA betroffen. Dies betrifft vorrangig Projekte, die in kommerziellen Produkten genutzt werden und durch die neue, vom CRA geschaffene Rolle des „Stewards“ Teil der Regulierung sein können.
Der Workstream widmete sich der Frage, wie der CRA die „Kultur“ innerhalb der Open Source Welt verändert, welche rechtlichen Anforderungen für die potenziell betroffenen unklar sind und welche Erwartung die einzelnen Akteure an eine künftig notwendige Zusammenarbeit aneinanderstellen und welche Bedürfnisse sie haben. Hierzu wurden sowohl Softwarehersteller, Open Source Projekte sowie potenzielle künftige Stewards anhand einer Onlinebefragung konsultiert.

Im Rahmen der Befragung ergaben sich drei Hauptfelder, welche den Akteuren als Herausforderungen im Rahmen der künftigen Zusammenarbeit und Implementierung des CRA erschienen. Gleichzeitig konnte die Befragung so auch potenzielle Lösungsansätze identifizieren:

1. Unklarheit von Rollen, Rechten und Pflichten, wie sie sich aus dem Gesetzestext ergeben.
   - Hier kann entsprechende Guidance durch die Kommission Rechtssicherheit schaffen.

2. Kulturunterschiede zwischen Herstellern und OSS-Projekten: Hersteller wünschen sich Sicherheit, OSS-Projekte möglichst wenig (extern verursachten) Aufwand.
   - Hier kann die Etablierung von Standards/Guidance, Tools und Best Practices helfen, kulturelle Unterschiede zu überbrücken.

3. Planungssicherheit: Die Etablierung funktionierender Kommunikationsstrukturen benötigt ebenso Planbarkeit wie das Verhindern der „Verwaisung“ von Projekten.
   - Dem kann entgegengewirkt werden, indem etwa langfristigere Fördermöglichkeiten geschaffen werden.

Im Folgenden einige Erkenntnisse im Detail:

- Der CRA birgt bisher noch Unklarheiten, insbesondere hinsichtlich der konkreten Voraussetzungen, welche Eigenschaften eine Tätigkeit als „kommerzielle Tätigkeit“ klassifizieren. Im Ergebnis entstehen für Open Source Entwickler oft die Unsicherheit, welche Anforderungen zu erfüllen sind.
    - Hier kann eine Konkretisierung durch die Guidance der Kommission Abhilfe verschaffen
- In der Befragung der Hersteller zeigte sich die Befürchtung, dass der CRA (selbst wenn Open Source Projekte selbst keine Pflichten erfüllen müssen) als Dämpfer für den Bereich Open Source wirkt und im Zweifel mehr (auch innerhalb der eigenen Produkte genutzte) Projekte "verwaisen".
    - Eine grundsätzliche Lösung wäre hier der "Fork" d.h. die selbstständige Weiterentwicklung durch den Hersteller. Im Rahmen der Befragung gab der überwiegende Teil der Hersteller an, dies aktuell nicht zu tun/ zu planen.
- Grundsätzlich zeigen sich Hersteller besorgt, ob eine Kommunikation mit den OSS-Projekten (etwa zur Behebung von Schwachstellen) effizient genug ablaufen kann, um die Anforderungen des CRAs an ihre eigenen Produkte zu erfüllen.
    - Aufgrund der bislang begrenzten Erfahrung lässt sich schwer einschätzen, ob die Bedenken der Hersteller berechtigt sind. Prinzipiell wurden jedoch Standards/ Best Practices/ Tools für einen Austausch (etwa der Meldung von Schwachstellen) als hilfreich angesehen.
- Aus Herstellersicht zeigte sich ein Interesse, an Formen der einfachen Identifizierung. Hiermit ist gemeint, dass Open Source Projekten, welche die Cybersicherheitsanforderungen des CRA erfüllen, einfacher auffindbar werden sollen. Für entsprechende Nachweise wären Hersteller auch bereit, Geld zu bezahlen.
- Potenzielle Stewards zeigten primär den Bedarf an, dass ihnen ihre Rolle klar und verständlich hinsichtlich ihrer Rechte und Pflichten dargelegt wird.
- Grundsätzlich, hoffen die potenziellen Stewards, ihre Rolle weniger als professionelle Tätigkeit (auch hinsichtlich Entlohnung) verstehen zu müssen und dass dies mit einem entsprechend geringen Aufwand einhergeht.

1. Einleitung

Mit dem Cyber Resilience Act (CRA) wird derzeit ein Gesetz implementiert, das die Voraussetzungen für die Entwicklung sicherer Produkte mit digitalen Elementen festlegen. Dabei soll sichergestellt werden, dass Hardware- und Softwareprodukte mit weniger Schwachstellen auf den Markt gebracht werden. Um dies zu realisieren sollen Hersteller die Sicherheit während des gesamten Lebenszyklus eines Produkts ernst nehmen. So werden Bedingungen geschaffen, die es Nutzenden ermöglichen, Cybersicherheit bei der Auswahl und Nutzung von Produkten mit digitalen Elementen zu berücksichtigen. Schlussendlich sollen die Produkte dann mit einem CE Label gekennzeichnet werden und die Durchsetzung der Konformität von Produkten, die auf dem EU-Markt verkauft werden, von Marktüberwachungen überprüft werden.

Eine entscheidende Rolle spielt, wie und wann Produkte auf den europäischen Markt gebracht werden. Hier gibt der „Blue Guide“ wie folgt Hilfestellungen. Die Bereitstellung eines Produkts auf dem Markt bedeutet jede entgeltliche oder unentgeltliche Abgabe eines Produkts zum Vertrieb, zum Verbrauch oder zur Verwendung auf dem Unionsmarkt im Rahmen einer gewerblichen Tätigkeit. Der Begriff „Bereitstellung“ bezieht sich auf jedes einzelne Produkt. Im Bereich Open Source Software wurden hierfür spezifische Rollen und Ausnahmen geschaffen, die bei der Implementierung Fragen und Probleme aufwerfen, die durch die Arbeit im Workstream adressiert wurden. Durch das Gesetz werden drei verschiedene Rollen eingeführt: Die Hersteller – die ein Produkt auf den Markt bringen wollen, die Stewards (Verwalter), welche die Freie Software, die in einem Produkt landet, verwalten und eine umfassende Ausnahme für alle jene, die Freie Software zur Verfügung stellen, um ihren Lebensunterhalt zu verdienen oder dies aus altruistischen Gründen tun.

Es zeigt sich, dass die Implementierung des CRA derzeit noch viele Fragen für die Betroffenen aufwirft und zu entsprechenden Diskussionen und Verunsicherungen führt.

Mit dem Workstream haben wir Erkenntnisse über den EU Cyber Resilience Act (CRA) und seine Auswirkungen erlangt und diese in den Diskussionsprozess um die Implementierung eingebracht. Dabei lag ein besonderer Fokus auf Unklarheiten im Bereich der jeweiligen Rollen und wie diese künftig interagieren.

2. Vorgehen

Das grundsätzliche Thema des Workstreams wurde im Rahmen der Ideenwerkstatt am 16.11.2024 festgelegt und die Workstream-Sprecher wurden per Abstimmung bestimmt. Den Workstream-Sprechern kam hierbei insbesondere die Rolle als Moderatoren innerhalb des Workstreams zuteil. Als offenes Community-Projekt wurde im Anschluss ein Aufruf zur Beteiligung über verschiedene Kanäle (offizielle Kommunikation des Dialogs für Cybersicherheit, Social-Media-Kanäle) verteilt.

Nach der Etablierung des Workstream-Teilnehmenden wurden monatliche Arbeitstreffen organisiert, im Rahmen derer das weitere Vorgehen sowie Arbeitsstände der aktuellen Arbeitspakete diskutiert wurden. Die Mitarbeit an den jeweiligen Arbeitspaketen geschah frei, d.h. jeweilige Vorschläge und Arbeitsdokumente wurden innerhalb des Workstreams geteilt, wodurch jedem Workstream-Teilnehmenden die Möglichkeit gegeben wurde, einen entsprechenden Beitrag zu leisten. Ergebnisse wurden entsprechend innerhalb des Workstreams zur Diskussion gestellt und gemeinsam finalisiert.

2.1. Projektplan

Der Workstream gliederte sich in neun, teils aufeinander aufbauende, Arbeitspakete (APs). Somit wurde zunächst zur fachlichen Vorbereitung eine Wissensgrundlage (siehe Kapitel 2.21) durch allgemeine und dezidiert rechtliche Recherche zur Auslegung des CRA erarbeitet. Kernstück des Workstreams waren die Vorbereitung, Durchführung und Auswertung einer Stakeholder-Befragung (siehe Kapitel 3.2). In den Arbeitspaketen Outreach und Dokumentation wurden die (bisherigen) Ergebnisse des Workstreams jeweils auf Veranstaltungen vermittelt, im Rahmen eigener Workshops Wissen von externen Experten eingeholt sowie festgehalten (siehe Kapitel 3.1).

Workstream Cybersicherheit in der Gesellschaft - die Rolle des CRA für Open Source

		2024	2025										
Workstream-Phase	**Arbeitsschritt**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**Mitarbeit**
		Dez	Jan	Feb	Mrz	April	Mai	Jun	Jul	Aug	Sep	Okt	
Erstellung Projektplan													
AP 1 Recherche	laufend												
AP 2 Stakeholderansprache													
AP 3 Fragebögen													
AP 4 Auswertung													
AP 5 CRA-Auslegung													
AP 6 EU-Begleitung (z. B. Expertenkommision)													
AP 7 Outreach						03.04.2025		11.06.2025			11.09.2025		
AP 8 Dokumentation													
AP 9 Wissensspeicher													

Agenda

- regulärer Plan
- Laufzeit verlängert
- optional

Abbildung 1.1

2.2. Arbeitspakte im Detail

2.2.1. Erstellung der Wissensgrundlage (AP 1 Recherche und AP 5 CRA-Auslegung)

Im Rahmen der Erstellung der Wissensgrundlage kam es zunächst darauf an, fachlich in das Thema CRA allgemein einzusteigen. Hierbei wurden Verständnis- und Auslegungsfragen innerhalb des Workstreams geklärt, um eine gemeinsame Basis für die nächsten APs zu schaffen. Ebenfalls wurden laufend aufkommende fachliche Fragen bearbeitet.

2.2.2. Vorbereitung und Durchführung der Stakeholderbefragung (AP 2 Stakeholder Ansprache, AP 3 Fragebögen, AP 4 Auswertung)

Kern des Workstreams war die Vorbereitung, Durchführung und Auswertung einer Stakeholderbefragung. Hierzu wurden zunächst potenzielle Stakeholder identifiziert. Im Rahmen der Erstellung der Fragebögen wurden bereits einzelne Stakeholder und Interessensgruppen kontaktiert und hinsichtlich ihrer Einschätzungen zu potenziell offenen Fragestellungen im Zusammenhang des CRAs befragt. Die Antworten wurden entsprechend in der Erstellung der Fragebögen berücksichtigt, welche innerhalb des Workstreams finalisiert wurden. Im Rahmen der Durchführung wurden die Fragebögen jeweils breit und unter Einbeziehung verschiedener Verbände und Gruppen, die bereits intensiv am CRA arbeiten, an potenzielle Stakeholder gestreut, und die Ergebnisse entsprechend ausgewertet.

2.2.3. Begleitende Öffentlichkeitsarbeit (AP 6 EU-Begleitung, AP 7 Outreach)

Die Ergebnisvermittlung und Öffentlichkeitsarbeit bestanden im Wesentlichen aus drei Teilen. Der erste Teil befasste sich explizit mit der Kommunikation mit der bei der EU-Kommission für die Erstellung der „CRA-Guidance“ zuständigen Stelle (CNECT). In verschiedenen Treffen sollten Unklarheiten im Zusammenhang mit der Auslegung des CRA ad hoc ausgeräumt werden und ein Kanal für die finale Ergebnisvermittlung an die Kommission geschaffen werden. Im Ergebnis soll so der Kommission ein Stimmungsbild aus der Open Source Community hinsichtlich offener Fragen und praktischer Herausforderungen bei der Umsetzung des CRA vermittelt werden, in der Hoffnung, dass dieser konstruktive Einfluss in die Formulierung der „CRA-Guidance“ findet.

Der zweite Teil befasste sich im Wesentlichen mit der Vorstellung von (Teil-)Ergebnissen auf entsprechenden Fachkonferenzen. Hierbei wurde sowohl Werbung Teilnahme an der Umfrage gemacht, als auch Feedback zu bisherigen Arbeitsständen eingeholt.

Der dritte Teil befasste sich mit einer Veranstaltungsreihe in deren Rahmen externe Speaker zum Thema CRA, im weitesten Sinne, eingeladen wurden (siehe Kapitel 3.1).

2.2.4. Dokumentation und Wissensspeicher

Begleitend zum Workstream wurden die entsprechenden Arbeitsstände und Ergebnisse dokumentiert und Workstream-intern in einer kollaborativen Arbeitsumgebung geteilt.

3. Ergebnisse

3.1. Ergebnisse der Öffentlichkeitsarbeit

Im Rahmen eigens organisierter Sessions wurden verschiedene Experten aus dem CRA Ökosystem zu virtuellen Vorträgen inkl. Diskussion eingeladen, um verschiedene Schwerpunkte zu diskutieren. Im Rahmen dieser Vortragsreihe fanden die folgenden Sessions statt:

- **03.04.2025, Maarten Aertsen, „The Role of Cyber Resilience Act (CRA) for Open Source“:** Maarten Aertsen's Vortrag konzentriert sich darauf, wie Free and Open Source Software (FOSS) im Cyber Resilience Act adressiert wird, insbesondere wie sich das von anderen Regelungen im Stil des New Legislative Framework (NLF) in verschiedenen Segmenten unterscheidet.
    - Die Aufnahme ist hier verfügbar: https://www.youtube.com/watch?v=l0PswtQ2p6M

- **11.06.2025 fukami (Christian Heuchert), „CRA - Now Wait for Last Year“:** Mit der Umsetzung des Cyber Resilience Act (CRA) und der aktiven Entwicklung europäischer Standards ist es an der Zeit, erste Schlussfolgerungen zu ziehen: Was ist geschehen, was war erfolgreich, welche potenziellen Herausforderungen könnten künftig entstehen und welche Fragen bleiben ungeklärt. fukami's Vortrag beleuchtet die Feinheiten eines der beeindruckendsten EU-Gesetze.
    - Die Aufnahme ist hier verfügbar: https://www.youtube.com/watch?v=pNXerXY7-bg

- **11.09.2025 Gergor Bransky, „Der Cyber Resilience Act – Auswirkungen auf die Mitgliedsstaaten“.**

Im Rahmen von Vorträgen auf Konferenzen wurde sowohl auf die Stakeholderbefragung aufmerksam gemacht, als auch vorläufige Ergebnisse vorgestellt. Folgende Vorträge fanden statt:

- **16.08.2025 FrOSCon auf dem Campus der Hochschule Bonn-Rhein-Sieg:** Alexander Sander und Michael Schuster, „Cybersicherheit in der Gesellschaft“
    - Die Aufnahme ist hier verfügbar: https://media.ccc.de/v/froscon2025-3318-cybersicherheit_in_der_gesellschaft

- **20.09.2025, Datenspuren des Dresdner Chaos Computer Clubs in Dresden:** Alexander Sander und Michael Schuster, „Cybersicherheit in der Gesellschaft“
    - Die Aufnahme ist hier verfügbar: https://talks.datenspuren.de/ds25/talk/SSPWGZ/

Die Aktivitäten in diesem Bereich ermöglichten zudem, mit weiteren Stakeholdern aber auch Entscheidungsträgern wie der Europäischen Kommission oder Marktüberwachungen ins Gespräch zu kommen. In einem Gespräch mit den verantwortlichen Vertretern der Europäischen Kommission wurde auch in Hinblick auf die Open Source Guidance zum CRA darauf hingewiesen, dass für viele Projekte unklar ist, ob sie ein Produkt im Sinne des CRA bereitstellen und ob sie eine Gewinnerzielungsabsicht haben. So wird sichergestellt, dass die Ergebnisse des Workstreams schlussendlich in der Implementierung des CRA aufgenommen und adressiert werden. Als Möglichkeit wurde hier der Verweis auf den „Blue Guide“ mit weiteren Erklärungen genannt und auch die Bereitstellung von Beispielen, um auf die Diversität des Open Source Ökosystems einzugehen.

Im Verlauf dieses Arbeitspakets des Workstreams konnte auch erkannt werden, dass sich weitere Fragen um die Attestierung von Open Source Komponenten nach CRA-Artikel 25 stellen. Eine Frage ist, wie diese Attestierungen, bzw. Bescheinigungen für Open Source genutzt werden können, um Projekten die Möglichkeit zu geben, nachzuweisen, dass sie bestimmte Anforderungen des CRA erfüllen. Herstellern könnte es helfen, ihre „Due Diligence“ gegenüber Open Source Komponenten nachzuweisen. Zudem wurde diskutiert, wie diese Bescheinigung konkret aussehen kann. In dieser Diskussion stellt sich auch die Frage der Finanzierung, vor allem in dem Bereich, der nicht von Foundations abgedeckt wird. Ähnlich wie bei der Stewardproblematik ergeben sich Verteilungsfragen, die adressiert werden müssen.

In den verschiedenen Treffen, die sich rund um den Outreach ergeben haben, wurde klar, dass sich intensiver mit diesen Fragestellungen befasst werden muss. Hierfür haben auch mehrere Workshopteilnehmer an einem Workshop mit der Eclipse Foundation (eine gemeinnützige Gesellschaft mit der Aufgabe, die Eclipse-Open-Source-Gemeinschaft und ihre Projekte zu unterstützen) teilgenommen, um einen besseren Einblick in die Debatte und aktuelle Herausforderungen erlangen zu können.

3.2. Ergebnisse der Stakeholder Befragung

3.2.1. Allgemeines

Im Rahmen dieses Workstreams wurden sechs Fragebögen (3x DE, 3x EN) erstellt. Bei der Erarbeitung der Fragen wurde breites Feedback, u. a. von OSS Projekten, der Open Source Business Alliance, der Linux Foundation und der Eclipse Foundation einbezogen. Die Laufzeit zur Beantwortung der Fragebögen betrug 2 Monate. Insgesamt gab es 345 Antworten auf Fragen des Fragebogens und 83 vollständig beantwortete Fragebögen.
In den Fragebögen wurde explizit darauf hingewiesen, dass nicht alle Fragen beantwortet werden müssen. Ziel war Qualität, nicht Quantität und dementsprechend war die inhaltliche Vertrautheit mit dem CRA entscheidend, nicht die bloße Zahl der Teilnehmenden mit diffusen Befürchtungen.
Übergreifend kann festgestellt werden, dass viele Stakeholder bisher nicht genau wissen, welche Rolle sie im CRA einnehmen werden. Vor allem die Steward Rolle ist bisher nicht klar definiert. Hier soll durch die Guidance Klarheit geschaffen werden. Wichtig ist zudem, Open Source Entwickler nicht mit Regulierungen zu überfordern, sondern sie weiter ihrer Arbeit nachgehen zu lassen – der Software-Entwicklung. Ein weiterer wichtiger Aspekt ist es, dass Hersteller wiederum Rechtssicherheit bei der Integration von Open Source Komponenten in ihre Produkte benötigen. Zudem braucht es, um den CRA umsetzen zu können, Tools (zur Prüfung, Meldung und Nachweisführung) für sämtliche Akteure sowie finanzielle Unterstützung für potentielle Stewards. So sollten Prozesse vereinfacht und praktikabel gemacht werden und Akteure in die Lage versetzt werden mehr Cybersicherheit erreichen zu können und gleichzeitig keinen Qualitätsverlust bei der eigentlichen Entwicklung zu riskieren.

In den folgenden Abschnitten wird genauer auf die spezifischen Stakeholdergruppen und ihre Perspektive eingegangen.

3.2.2. Ergebnisse der Herstellerbefragung

Die Herstellerbefragung gibt Aufschluss darüber, wie Unternehmen die Anforderungen und Folgen des Cyber Resilience Act (CRA) einschätzen. Die Auswertung konzentriert sich auf drei zentrale Fragestellungen:

- Welche wesentlichen Unklarheiten bestehen auf Seiten der Hersteller?
- Welche zusätzlichen Aufwände und welche Rolle der Stewards werden erwartet?
- Welche Ideen bestehen, um das Zusammenspiel innerhalb der Open Source Community zu verbessern?

1. Wesentliche Unklarheiten mit dem CRA aus Herstellersicht

Die Antworten verdeutlichen, dass Hersteller zwar bemüht sind, die CRA-Vorgaben zu verstehen, jedoch in mehreren Bereichen Unsicherheit herrscht.

1.1 Verantwortung und Anwendbarkeit auf Open Source

Viele Hersteller wissen nicht, in welchem Umfang Open Source Projekte selbst unter den CRA fallen. Sie sehen Widersprüche zwischen der offenen, gemeinnützigen Entwicklung und den produktbezogenen Pflichten des CRA. Unklar ist insbesondere die **Abgrenzung der Verantwortlichkeiten**:

- Liegt die Pflicht bei den Herstellern, die OSS integrieren,
  - „Soweit wir den CRA verstanden haben, fallen Open Source Projekte nicht unter die CRA-Regeln."
- oder auch bei den Projekten bzw. Stewards, die Komponenten bereitstellen?
  - „Am Ende müssen die Produkte die CRA-Anforderungen erfüllen."

Kernproblem: Fehlende Klarheit über juristische Zuständigkeiten und den Anwendungsbereich des CRA auf OSS-Ebene.

1.2 Nachweisführung und technische Umsetzbarkeit

Hersteller sind unsicher, wie die CRA-Konformität in der Praxis nachgewiesen werden soll – insbesondere bei einer Vielzahl eingesetzter Open Source Komponenten. Es fehlen **klare Vorgaben und geeignete technische Verfahren**, um Compliance-Prüfungen zu automatisieren.

- „Für alle Komponenten die Erfüllung von Anhang I (Anmerkung: Gemeint ist der erste Anhang des CRA) sicherzustellen, ist weltfremd – der Aufwand wäre absurd hoch."

Kernproblem: Fehlende technische und organisatorische Leitlinien für den Nachweis der CRA-Konformität.

1.3 Rolle und Finanzierung von Stewards

Unklar ist, wer künftig die Rolle eines Stewards übernimmt und wie Aufgaben, anfallende Kosten und Zuständigkeiten verteilt werden. Hersteller wissen nicht, ob eine finanzielle Beteiligung verpflichtend oder freiwillig ist.

- „Idealerweise zahlen Hersteller … einen Beitrag, der den Projekten zugutekommt."
- „Viele Hersteller arbeiten noch gar nicht mit potenziellen Stewards zusammen."

Kernproblem: Fehlende Modelle zur Rollenverteilung und Kostenteilung zwischen Industrie und Open Source Projekten.

1.4 Rechtliche Unsicherheiten

Einzelne Hersteller äußern Unsicherheit hinsichtlich Haftung, Lizenzbedingungen und Vertragsgestaltung. Unklar bleibt, ob neue Vertragsformen mit Stewards oder Foundations notwendig werden.

Kernproblem: Fehlende rechtliche Orientierung zu Haftung, Vertragsfragen und Nachweisverpflichtungen.

1.5 Langzeitpflege und Sicherheitsunterstützung

Die Vorgabe, Sicherheitsupdates über viele Jahre zu gewährleisten, wird als kaum umsetzbar beschrieben. Da Open Source Projekte selten langfristigen Support leisten, ist unklar, ob Hersteller diese Verantwortung selbst übernehmen müssen.

- „Security Support Period von 10 bis 15 Jahren."
- „Von Freiwilligen verfolgte Projekte können kein Commitment zur langfristigen Pflege aufbringen."

Kernproblem: Fehlende Klarheit über Dauer und Verantwortlichkeit der Sicherheitsunterstützung.

1.6 Zusammenfassende Bewertung

Themenfeld	Beschreibung der Unklarheit
Anwendbarkeit des CRA auf OSS	Ob und wann Open Source Projekte selbst unter den CRA fallen
Nachweisführung	Wie CRA-Konformität nachgewiesen werden kann
Rolle der Stewards	Zuständigkeiten und Finanzierung
Rechtliche Verantwortung	Haftung, Verträge, Lizenzfragen
Langzeitpflege	Sicherstellung langfristiger Sicherheitsunterstützung

Fazit: Der CRA wird von Herstellern vor allem als organisatorische und juristische Herausforderung wahrgenommen. Unklarheiten bestehen insbesondere bei der Verantwortungsteilung, der Nachweisführung und der langfristigen Sicherheitspflege.

2. Erwartete Zusatzaufwände und zukünftige Rolle der Stewards

Hersteller rechnen mit deutlichen Mehrbelastungen, insbesondere durch neue Dokumentations-, Nachweis- und Organisationspflichten sowie die Aufwände zur Erfüllung der in CRA Anhang I aufgeführten Sicherheitsanforderungen.

2.1 Nachweis- und Dokumentationspflichten

Die Erfüllung der CRA-Vorgaben erfordert den Aufbau von Prozessen, die Sicherheitsprüfungen, Versionskontrolle und Updates systematisch erfassen. Mehrere Antworten betonen die Notwendigkeit von Automatisierung und technischem Tooling, um den Aufwand beherrschbar zu halten.

Zusatzaufwand: Aufbau neuer Compliance-Systeme und automatisierter Prüfroutinen.

2.2 Langzeitpflege und Sicherheits-Updates

Die Verpflichtung zu langfristiger Sicherheitspflege gilt als kaum realisierbar. Hersteller erwarten zusätzliche Ressourcen für Wartung, ggf. eigene Forks oder interne Supportteams.

Zusatzaufwand: Langfristige Wartungs- und Sicherheitskosten.

2.3 Lizenz- und Compliance-Management

Der CRA verstärkt die Notwendigkeit eines systematischen Lizenz- und Schwachstellenmanagements (SBOM, CVE). Dies erfordert organisatorische und juristische Anpassungen in den Entwicklungsprozessen.

Zusatzaufwand: Ausweitung interner Compliance- und Rechtsprüfungen.

2.4 Kommunikation und Governance

Die Zusammenarbeit mit Open Source Projekten wird komplexer. Hersteller müssen künftig Abstimmungs- und Reporting-Strukturen etablieren, um CRA-relevante Informationen nachzuhalten.

Zusatzaufwand: Erhöhter Koordinationsbedarf mit der OSS-Community.

2.5 Rechtliche und vertragliche Anpassungen

Hersteller erwarten zusätzliche Aufwände für juristische Beratung und Vertragsmanagement, um Pflichten gegenüber Stewards und Zulieferern klar zu regeln.

Zusatzaufwand: Rechtsberatung, Standardverträge, interne Richtlinien.

2.6 Rolle der Stewards aus Herstellersicht

Die Hersteller erwarten, dass Stewards künftig:

- Nachweise über die CRA-Konformität einzelner Komponenten erbringen,
- bei Sicherheitsfragen koordinierend tätig sind,
- und eine Mittlerrolle zwischen Community und Industrie übernehmen.

Damit werden Stewards aus Sicht vieler Unternehmen zu **verantwortlichen Partnern** für Sicherheit und Nachvollziehbarkeit in der Open Source Lieferkette.

3. Verbesserung des Zusammenspiels in der Open Source Community
Hersteller formulieren mehrere Ansätze, um die Zusammenarbeit mit der Community zu stärken:

- **Einheitliche Standards:** Gemeinsame Sicherheits- und Compliance-Regeln sollen den Austausch erleichtern.
    - „Die Community sollte sich abgestimmten Regeln unterwerfen."
- **Institutionalisierte Kooperation:** Kooperationen über bestehende Organisationen wie Foundations werden bevorzugt, um Governance und Kommunikation zu bündeln.
- **Finanzielle Unterstützung:** Hersteller befürworten Förder- und Beteiligungsmodelle, um sicherheitskritische Projekte zu stabilisieren.
    - „Ein Beitrag, der den Projekten zugutekommt."
- **Technische Zusammenarbeit:** Gemeinsame Tools zur Prüfung, Meldung und Nachweisführung sollen Doppelarbeit vermeiden.

Fazit: Hersteller wünschen sich eine stärker strukturierte und institutionalisierte Zusammenarbeit mit Open Source Projekten. Dabei sollen **gemeinsame Standards, finanzielle Unterstützung und klare Kommunikationswege** die Grundlage bilden, um CRA-Anforderungen wirksam und partnerschaftlich umzusetzen.

Gesamtbewertung: Die Hersteller sehen den CRA als Impuls, die Zusammenarbeit zwischen Wirtschaft und Open Source neu zu organisieren. Die zentrale Herausforderung liegt weniger in der Technik, als in der **klaren Zuweisung von Verantwortung, Finanzierung und Nachweisprozessen**.

3.1. Erwartete Zusatzaufwände durch den CRA und zukünftige Rolle der Stewards

Hier geht es darum, **was Hersteller an zusätzlichem Aufwand durch den CRA erwarten** und **welche Rolle die Stewards** künftig aus Sicht der Industrie spielen sollen.

Die Ergebnisse hier basieren auf allen ausgewerteten Herstellerangaben aus den Fragen 16–28.

3.1.1. Erwartete Zusatzaufwände durch den CRA

Hersteller rechnen mit **spürbaren Mehraufwänden**, vor allem in den Bereichen **Dokumentation, Nachweis, Organisation und Langzeitpflege**. Die folgenden Punkte wurden in mehreren Antworten explizit oder indirekt benannt:

A. Nachweis- und Dokumentationspflichten

- „Für alle Komponenten die Erfüllung von Anhang I sicherzustellen, ist weltfremd – der Aufwand wäre absurd hoch." „Ein Nachweis müsste … durch vollständig automatisiertes Tooling erbracht werden."
- **Erstellung, Pflege und Aktualisierung von CRA-Nachweisen für jede OSS-Komponente.**
- Aufbau von **internen oder externen Prozessen**, um Sicherheitsprüfungen, Versionskontrolle und Update-Status kontinuierlich nachzuhalten.
- **Automatisierung und Tooling erforderlich, um Aufwand beherrschbar zu machen.**

Aufwand: Aufbau neuer Compliance-Systeme und automatisierter Prüfroutinen.

B. Langzeitpflege und Sicherheits-Updates

- „Security Support Period von 10 bis 15 Jahren." „Von Freiwilligen verfolgte Projekte können kein Commitment zur langfristigen Pflege aufbringen."
- **Verlängerung der Produktverantwortung: Hersteller müssen langfristig Sicherheitsupdates garantieren, auch wenn OSS-Projekte diese einstellen.**
- Einrichtung von **internen Wartungsteams** oder **eigene Forks** für verwaiste OSS-Komponenten.

Aufwand: Langfristige Wartungs- und Sicherheitskosten, die bisher nicht eingeplant waren.

C. Lizenz- und Compliance-Management

- „Lizenzänderung während der Nutzungsdauer", „Nicht-lizenzkonforme Nutzung durch Lieferanten."
- **Erweiterte Prüfungspflichten entlang der Lieferkette (Third-Party-Compliance, Lizenzkonformität, SBOM).**
- Integration von **CVE-Management** und **Lizenztracking** in Entwicklungs- und Releaseprozesse.

Aufwand: Organisatorische und juristische Compliance-Arbeit.

D. Kommunikation und Governance

- „Es ist sehr schwierig, alle Projekt-Repositories zu kontaktieren.“ „Ein Mechanismus, der eine positive CRA-Bewertung durch Dritte auch wieder an die Community zurückspielt.“
- Aufbau von **Kooperationsstrukturen mit Open Source Projekten**, um Sicherheitsfragen, Nachweise oder Audits abzustimmen.
- Erhöhter **Koordinationsaufwand mit Communitys**, die bislang unabhängig agierten.

Aufwand: Mehr Zeit und Ressourcen für Abstimmung, Reporting und Informationsfluss.

E. Rechtliche und vertragliche Klarheit

- „Eine Unterstützung für rechtliche Beratung wäre wichtig.“ „Wer haftet, wenn eine OSS-Komponente nicht CRA-konform ist?“
- Klärung von **Haftung, Lizenz und Vertragsverhältnissen** zwischen Herstellern, Zulieferern, Stewards und Open Source Projekten.
- Möglicherweise **juristische Beratung** oder Standardverträge erforderlich.

Aufwand: Rechtsberatung, Vertragsmanagement, interne Richtlinien.

3.1.2. Erwartete zukünftige Rolle der Stewards

In den Antworten zu den Fragen 22-27 zu der zukünftigen Rolle der Stewards entsteht ein konsistentes Bild: Hersteller erwarten, dass **Stewards eine neue Mittlerrolle** zwischen Open Source und Industrie übernehmen.

A. Prüfinstanz und Nachweisdienstleister

- „Die Stewards stellen einen Nachweis der CRA-Erfüllung zur Verfügung, den wir automatisiert verarbeiten.“ „Steward kann sicherstellen, dass [die] Komponente sicher ist und das zertifizieren.“
- Stewards sollen **CRA-Konformität prüfen, dokumentieren und zertifizieren**.
- Hersteller möchten **diese Nachweise übernehmen**, anstatt eigene Prüfungen für jede Komponente zu machen.
- Ziel: **Zentralisierte, wiederverwendbare Nachweise** für viele Projekte.

Rolle: Prüfstelle für CRA-Compliance; **ähnlich einer Zertifizierungsstelle** in der Lieferkette.

B. Schnittstelle zwischen Industrie und Community

- „beispielsweise über Gremien wie die Eclipse Foundation …“ „Ein Mechanismus, der eine positive CRA-Bewertung … an die Community zurückspielt.“
- Stewards sollen **Kommunikationsbrücken** schaffen – zwischen freiwilligen OSS-Communities und industriellen Nutzern mit Compliance-Pflichten.
- Sie könnten **Best-Practice-Prozesse und CRA-Regeln** in die OSS-Entwicklung einführen.

Rolle: Koordinations- und Übersetzerfunktion zwischen Community und regulierter Industrie.

C. Finanzierungs- und Unterstützungsrolle

- „Idealerweise zahlen Hersteller einen Beitrag, der den Projekten zugutekommt.“ „Finanzielle Unterstützung, Sponsoring, Mitarbeit.“
- Stewards könnten **Zuwendungen oder Lizenzbeiträge verwalten**, um Pflege und Zertifizierung von Projekten zu finanzieren.
- Damit entstehen **nachhaltige Finanzierungsmechanismen** für sicherheitskritische OSS-Komponenten.

Rolle: Treuhänder und Förderpartner für die finanzielle und organisatorische Stabilität von OSS-Projekten.

D. Flexible Verantwortungsteilung

- „Hersteller sollten die Freiheit haben, die Sicherheit von OSS-Komponenten entweder selbst herzustellen oder mit Stewards zusammenzuarbeiten.“
- Hersteller wünschen sich **Wahlfreiheit**, ob sie
    - CRA-Nachweise selbst erbringen oder
    - die Verantwortung vertraglich an Stewards delegieren.

Rolle: Optionale Compliance-Partner, nicht verpflichtende Institutionen.

Bereich	Erwarteter zusätzlicher Aufwand	Rolle der Stewards laut Herstellern
Nachweisführung	Aufbau neuer Compliance-Systeme, automatisierte Prüfungen	Prüfen und Zertifizieren von OSS-Komponenten
Langzeitpflege	Eigenwartung oder Forks für abgekündigte Projekte	Unterstützung durch Stewards bei Pflege und Sicherheit
Recht & Compliance	Juristische Klärung, Verträge, Beratung	Bereitstellung standardisierter, rechtssicherer Nachweise
Koordination & Kommunikation	Mehr Aufwand für Abstimmung mit Projekten	Vermittlung zwischen OSS-Community und Industrie
Finanzierung	Beiträge oder Sponsoring	Verwaltung von Mitteln zur CRA-konformen Weiterentwicklung

Bewertung: Der CRA wird aus Herstellersicht vor allem organisatorische, dokumentarische und rechtliche Mehrarbeit erzeugen. Stewards sollen künftig als Mittler, Prüfinstanz und Finanzierungsplattform fungieren – um CRA-Konformität in der Open Source Welt praktikabel, überprüfbar und nachhaltig zu gestalten.

3.2. Verbesserung des Zusammenspiels mit der Open Source Community

Dies zielt auf die **Gestaltung der zukünftigen Zusammenarbeit zwischen Herstellern und der Open Source Community** ab, wie sie aus den bisherigen Antworten herauslesbar ist.

Basierend auf den Antworten in den Fragen 16-27 (insbesondere 17, 22, 25, 26 und 27) zu der Verbesserung des Zusammenspiels von Open Source Community lassen sich **mehrere konkrete Ideen und Vorschläge** der Hersteller erkennen, wie dieses aussehen könnte.

3.2.1. Übersicht: Welche Intention steckt hinter den Aussagen?

Befragte Hersteller äußern **Respekt und Anerkennung** gegenüber der Open Source Community, sehen aber gleichzeitig **Defizite in Kommunikation, Nachweisführung und Struktur**. Ihre Vorschläge zielen darauf ab, das **Verständnis zwischen industriellen Anforderungen (CRA, Compliance, Haftung)** und **offener, freiwilliger Entwicklungskultur** zu überbrücken.

3.2.2. Ideen und Vorschläge der Hersteller

A. Einheitliche Regeln und gemeinsame Standards *(Frage 25)*

- „Die Community sollte sich abgestimmten Regeln unterwerfen."
- „Ein Mechanismus, der eine positive CRA-Bewertung durch Dritte auch wieder an die Community zurückspielt." *(Frage 25)*

Idee:

- Aufbau gemeinsamer **Sicherheits- und Compliance-Standards** in der OSS-Community.
- **Feedback-Schleifen: Wenn ein Projekt durch einen Steward oder Dritten geprüft wurde, sollen die Ergebnisse zurück an die Community fließen.**
- Ziel ist, **Lerneffekte und Qualitätssicherung** für alle Beteiligten zu schaffen.

Beitrag zur Verbesserung: Mehr Transparenz, gemeinsame CRA-Regeln, Rückkopplung von Auditergebnissen.

B. Institutionalisierte Kooperation über Foundations oder Stewards *(Fragen 26 und 27)*

- „beispielsweise über Gremien wie die Eclipse Foundation o. ä."
- „Stewards können ihre Projekte attraktiver für kommerzielle Verwender machen, indem sie CRA-Regeln einhalten."

Idee:

- Nutzung bestehender **Open Source Organisationen (Eclipse, Linux Foundation etc.)** als Mittler.
- Aufbau eines **verlässlichen Governance-Rahmens** für industrielle Zusammenarbeit.
- Stewards oder Foundations sollen **Standardprozesse für CRA-Nachweise** anbieten.

Beitrag zur Verbesserung: Vertrauensaufbau, strukturierte Kommunikation, Vermeidung von Einzelkontakten.

C. Finanzielle und organisatorische Unterstützung der Community *(Frage 25)*

- „Ein Mix – Übernahme kritischer Kernkomponenten durch Stewards oder andere Organisationen, Sponsoring und Förderung."
- „Für Projekte sollte es einen sehr einfachen Weg geben, das Einhalten der Anforderungen nachweisbar zu machen und dafür vergütet zu werden."

Idee:

- Einführung von **Förder- und Finanzierungsmodellen** für OSS-Projekte, insbesondere für sicherheitskritische oder systemrelevante Komponenten.
- Hersteller sollen **Beiträge leisten**, die direkt in Pflege, Dokumentation und Zertifizierung fließen.
- Stewards oder Foundations können als **Treuhänder** dieser Mittel fungieren.

Beitrag zur Verbesserung: Langfristige Stabilität der Projekte, Stärkung der Pflege- und Sicherheitsstrukturen.

D. Technische Kooperation und gemeinsame Werkzeuge *(Fragen 25 und 27)*

- „Der Nachweis ist jederzeit aktuell zu halten."
- „Ein Tool, das die Sicherheit von Open Source Komponenten CRA-konform sicherstellt."

Idee:

- Aufbau gemeinsamer **Tooling-Plattformen** für Compliance, CVE-Management und Nachweisautomatisierung.
- Ziel: **Automatisierte, gemeinschaftlich nutzbare Systeme**, um CRA-Compliance effizient zu erfüllen.

Beitrag zur Verbesserung: Weniger Doppelarbeit, mehr technische Effizienz, gemeinsamer CRA-Nachweis-Standard.

E. Gegenseitige Unterstützung und Rollenverständnis *(Frage 26)*

- „OSS-Community bittet Hersteller um Bereitstellung der Zertifizierungen …"
- „Auch ein ‚Outsourcing' von Qualifizierungsmaßnahmen an Hersteller … könnte denkbar sein."

Idee:

- Offenheit für **gegenseitige Unterstützung:**
  - Hersteller helfen mit **Zertifizierungen, Infrastruktur und Know-how**,
  - OSS-Projekte liefern **Transparenz und Sicherheitsinformationen**.
- Stärkung der **gemeinsamen Verantwortungskultur** statt Trennung in „Community" und „Industrie".

Beitrag zur Verbesserung: Partnerschaftliches Modell statt Pflichtenübertragung, gemeinsames Sicherheitsziel.

F. Realistische Erwartungshaltung und selektive Förderung *(Fragen 17 und 27)*

- „Es wird eine Zweiklassengesellschaft im Open Source etabliert …"
- „CRA wird zu einer Konzentration auf ausgewählte, industrienahe Projekte führen."

Idee:

- Hersteller erwarten, dass **nicht alle OSS-Projekte CRA-konform sein können**.
- Fokus auf **stabile, industrieunterstützte Kernprojekte** (Linux, OpenSSL, etc.).
- Förderung gezielter „CRA-ready"-Projekte, während kleinere Community-Projekte ggf. außen vor bleiben.

Beitrag zur Verbesserung: Fokussierung der Ressourcen, aber auch Risiko einer geringeren Diversität.

3.2.3. Gesamtbild

Hersteller schlagen keine grundlegend neuen Strukturen vor, sondern wünschen sich ein **koordiniertes, institutionelles Zusammenspiel** mit klaren Rollen:

Bereich	Erwartete Verbesserung	Beispielhafte Aussage
Regeln & Standards	Einheitliche CRA-konforme Prozesse	„Community sollte sich abgestimmten Regeln unterwerfen."
Koordination	Zusammenarbeit über Foundations	„bspw. Eclipse Foundation …"
Finanzierung	Hersteller unterstützen OSS-Projekte gezielt	„Beitrag, der den Projekten zugutekommt."
Tooling & Nachweise	Gemeinsame Tools und Automatisierung	„Tool, das Sicherheit von OSS-Komponenten sicherstellt."
Gegenseitige Hilfe	Austausch von Zertifikaten, Wissen, Infrastruktur	„Outsourcing von Qualifizierungsmaßnahmen an Hersteller."

Fazit: Aus Herstellersicht sollte das Zusammenspiel mit der OSS-Community künftig geprägt sein durch:

- Gemeinsame Standards und transparente Nachweisprozesse, um CRA-Anforderungen konsistent umzusetzen.
- Stewards oder Foundations als organisatorische Brücken, die Prüfung, Kommunikation und Finanzierung bündeln.
- Finanzielle Beteiligung der Industrie, um Sicherheit, Pflege und Langzeitstabilität von OSS zu sichern.

- Gegenseitige Unterstützung statt Abgrenzung – Hersteller und Community ergänzen sich in Verantwortung und Expertise.
- Pragmatische Fokussierung auf zentrale, gut gepflegte Projekte, ohne die Offenheit der OSS-Kultur zu gefährden.

Kurz gesagt: Hersteller, die den Beitrag der Stewards und der OSS-Community schätzen, wünschen sich für das CRA-Zeitalter eher ein **partnerschaftliches, strukturiertes und nachhaltiges Miteinander** mit der Open Source Community – getragen von **gemeinsamen Standards, fairer Finanzierung und gegenseitiger Verantwortung**.

3.2.3. Ergebnisse der Befragung der Stewards

Die Befragung der Stewards zeigt, wie Vertreter von Open Source Projekten ihre Rolle im Kontext des Cyber Resilience Act (CRA) einschätzen. Die Auswertung stützt sich auf die Antworten aus den Fragen 06–19 und behandelt drei zentrale Themenkomplexe:

- Wie sehen Stewards ihre Rolle in der Open Source Community, und wie verändert der CRA ihre Situation?
- Welche CRA-Anforderungen werden als zusätzlich wahrgenommen, und wie bewerten Stewards ihre Erfüllbarkeit?
- Wie kann die Zusammenarbeit zwischen Stewards, Herstellern und weiteren Akteuren verbessert werden?

1. Selbstverständnis und Veränderungen durch den CRA

1.1 Selbstverständnis der Stewards in der OSS-Community

Die Antworten verdeutlichen ein konsistentes Selbstbild der Stewards. Sie verstehen sich als **Verantwortliche und Koordinatoren**, die langfristig die **technische Stabilität, Sicherheit und Pflege** von Open Source Projekten gewährleisten. Die Steward-Rolle wird nicht als neue Funktion, sondern als **formalisierte Anerkennung bereits bestehender Verantwortlichkeiten** interpretiert.

Typische Aussagen lauten:

- „Übernahme der Verantwortung für die langfristige Pflege eines Projekts."
- „Systematically providing support on a sustained basis for the development of the product." „Durch Tun (beitragen), lehren, unterstützen."

Kernaussage: Stewards sehen sich als **vermittelnde Akteure** zwischen freier Open Source Entwicklung und regulierten industriellen Prozessen. Sie verbinden **technische Kompetenz, Freiwilligkeit und Kontinuität** mit dem Anspruch, als verlässliche Partner wahrgenommen zu werden.

1.2 Wahrgenommene Veränderungen durch den CRA

Die Einführung des CRA wird von den Stewards als einschneidend wahrgenommen. Sie erwarten eine Verschiebung von Verantwortung und eine stärkere Institutionalisierung ihrer Rolle.

A: Zunahme formaler Verantwortung

Der CRA überträgt Stewards indirekt eine **institutionalisierte, qualitätssichernde Rolle**. Sie werden nicht mehr nur als Entwickler, sondern als **Verantwortungsträger** in regulatorischen Zusammenhängen gesehen. Mehrere Antworten verweisen auf die

Sorge vor **haftungsähnlichen Verpflichtungen**.

- „The CRA unrealistic [sic!] perfection goals."
- „If becoming a steward is not an obligation that follows from CRA, I'd try to avoid it."

B: Erwartung steigender Anforderungen
Stewards rechnen mit einem deutlichen **Anstieg an Bürokratie, Dokumentations- und Nachweispflichten**. Gleichzeitig sehen sie die Möglichkeit, dass ihre Arbeit künftig stärker wahrgenommen und institutionell verankert wird.

C: Chancen durch Professionalisierung
Ein Teil der Befragten versteht den CRA als **Impuls zur Professionalisierung** von Open Source Strukturen. Genannt werden:

- die Entwicklung gemeinsamer Standards,
- der Aufbau stabiler Finanzierungsmodelle,
- und eine engere Kooperation mit Herstellern und Behörden.

Zugleich besteht die Sorge, dass eine zunehmende Formalisierung **den offenen Charakter von Open Source verändern** könnte.

1.3 Wahrgenommene Chancen und Risiken

Kategorie	Beschreibung	Beispielhafte Aussage
Anerkennung und Sichtbarkeit	Stewards werden als zentrale Akteure der digitalen Sicherheit wahrgenommen	„We build and maintain libraries used in commercial products. "
Professionalisierung	Aufbau von Strukturen, Tools und Prozessen zur nachhaltigen Projektpflege	„We'll have to find funding first. If we can find that, yes, we'll consider it."
Kooperation mit Industrie	Möglichkeit zu dauerhaften Partnerschaften mit Herstellern	„From manufacturers: Support (money and/or appropriately skilled people)."
Überlastung	Befürchtung wachsender Bürokratie und Belastung kleiner Projekte	„There is no funding yet, so that needs to come from somewhere."
Haftung und Verantwortung	Unsicherheit über juristische Risiken und Versicherungsbedarf	„A liability insurance that can take over the risk."
Abhängigkeit von Herstellern	Sorge, dass OSS-Projekte wirtschaftlich abhängig werden	„Payment is not part of the CRA at all (...)"

Fazit: Die Stewards sehen im CRA sowohl **eine Chance zur Stärkung ihrer Rolle,** als auch **das Risiko der Überforderung**. Sie befürworten eine Professionalisierung, fordern jedoch **klare Zuständigkeiten, faire Finanzierung und realistische Anforderungen**.

2. Wahrnehmung zusätzlicher CRA-Anforderungen und deren Erfüllbarkeit

2.1 Neue oder verstärkte Anforderungen

Mehrere Anforderungen des CRA werden als **neu oder deutlich verschärft** wahrgenommen. Die Befragten nennen insbesondere folgende Bereiche:

CRA-Anforderung	Wahrnehmung durch Stewards	Quelle
Nachweis der CRA-Konformität	Unklar, wie Nachweise zu erbringen sind; Wunsch nach einfachen Verfahren (z. B. Self-Assessment, SBOMs)	Frage 13
Schwachstellenmanagement	Reaktions- und Meldepflichten organisatorisch schwer umsetzbar	Frage 14
Langzeitpflege und Sicherheitssupport	Vorgesehene Supportdauer von 10–15 Jahren als unrealistisch angesehen	Fragen 09–10
Ressourcen- und Haftungsfragen	Mehr Personal, Finanzierung und Versicherung erforderlich	Fragen 10, 18
Koordination mit Behörden und Herstellern	Neue Kommunikations- und Dokumentationspflichten	Fragen 18–19

2.2 Einschätzung der Erfüllbarkeit

Die Einschätzungen sind geteilt: Etwa die Hälfte der Antwortenden hält die Erfüllung der CRA-Anforderungen für **grundsätzlich möglich**, wenn entsprechende **Unterstützung und Werkzeuge** bereitgestellt werden. Die andere Hälfte äußert **Zweifel an der praktischen Umsetzbarkeit**, insbesondere wegen fehlender Zuständigkeiten, Standards und Ressourcen.

- „That's up to the manufacturers to determine, not the steward."
- „Hierfür müssen entsprechende Prozesse und Tools etabliert werden."

2.3 Wahrgenommene Schwierigkeiten

Schwierigkeit	Beschreibung	Beispielhafte Aussage
Unklare Zuständigkeit	Unklar, wer (Hersteller oder Steward) rechtlich verantwortlich ist	„That's up to the manufacturers …“
Fehlende Infrastruktur	Keine etablierten Prozesse oder Tools für Nachweise und Meldungen	„Better tools for SBOM management …“
Zeitdruck	Kurze Fristen für Umsetzung und Meldung	„Bitte Plattformen früher in (Test-)Betrieb nehmen.“
Finanzielle Belastung	Keine Mittel für zusätzliche Sicherheits- oder Compliance-Aufgaben	„Faire Entlohnung für die Aufwände.“
Überforderung kleiner Projekte	Freiwillige Strukturen können neue Pflichten kaum erfüllen	„All of them. There is no funding yet (…)“

2.4 Bewertung der Erfüllbarkeit

Die Befragten betonen, dass CRA-Vorgaben nur **unter klar definierten Rahmenbedingungen und externer Unterstützung** umsetzbar sind. Fehlende Klarheit, fehlende Ressourcen und unzureichende technische Hilfsmittel gelten als Haupthindernisse. Kleinere Projekte sehen sich besonders gefährdet, die neuen Pflichten nicht einhalten zu können.

Gesamtbewertung: Die CRA-Vorgaben werden als **realistisch, nur bei zusätzlicher finanzieller, technischer und organisatorischer Unterstützung** angesehen.

3. Verbesserung der Zusammenarbeit aus Stewardsicht

In mehreren Antworten finden sich Hinweise, wie das Zusammenspiel zwischen Stewards, Herstellern, Behörden und der weiteren Open Source Community verbessert werden kann. Im Gegensatz zu den Herstellerantworten betonen die Stewards weniger den Aufbau neuer Strukturen, sondern die **Verbesserung bestehender Kooperationen** durch **gegenseitige Unterstützung, realistische Erwartungen und gemeinsame Werkzeuge**.

3.1 Gegenseitige Unterstützung und faire Arbeitsteilung

Stewards betonen, dass CRA-Compliance nur **gemeinsam mit Herstellern und Behörden** erreichbar ist. Erwartet wird keine einseitige Pflichtenübertragung, sondern ein **partnerschaftliches Vorgehen**.

- „The question is not: What do we need. The question is: What can we provide them with. Until we help the developers, the whole thing will not fly."
- „From manufacturers: Support (money and/or appropriately skilled people)."

Diese Aussagen verdeutlichen das Bedürfnis nach einer **gerechten Lastenteilung** zwischen Industrie und Open Source Akteuren.

3.2 Realistische Erwartungen und Freiwilligkeit

Mehrere Stewards warnen vor überhöhten Erwartungen der Industrie und Behörden. Sie fordern **Freiwilligkeit statt Zwang** bei der Übernahme von Steward-Rollen und **Respekt vor den begrenzten Ressourcen** freiwilliger Entwickler.

- „If becoming a steward is not an obligation that follows from CRA, I'd try to avoid it."
- „This is defective and can't be sustained."

Kooperation wird nur dann als tragfähig angesehen, wenn sie **auf Augenhöhe und mit realistischen Zielen** erfolgt.

3.3 Kommunikation, Transparenz und technische Unterstützung

Stewards betonen die Notwendigkeit klarer Kommunikations- und Meldewege, insbesondere bei Sicherheitsfragen.

- „Send security bug reports to the documented contact points, ideally with proposed fixes."

Darüber hinaus wünschen sie sich:

- **gemeinsame Tools und Infrastruktur zur Verwaltung von Schwachstellen und SBOMs,**
- **Schulungen und Orientierung durch Behörden,**
- und eine **offene, kontinuierliche Kommunikation** zwischen allen Beteiligten.

Diese Forderungen zielen auf **praktische, nicht bürokratische Verbesserungen** der Zusammenarbeit.

3.4 Strukturelle und finanzielle Unterstützung

Die Mehrheit der Stewards bejaht, dass **Hersteller die Arbeit der Stewards aktiv unterstützen müssen** – finanziell, personell und organisatorisch. Dabei geht es nicht um Bezahlung einzelner Nachweise, sondern um **nachhaltige Förderung des Open Source Ökosystems**.

- „Faire Entlohnung für die Aufwände."
- „Whatever helps to build a healthy Open Source ecosystem."
-

3.5 Institutionalisierte Vermittlung und Governance

Einzelne Antworten sprechen sich für koordinierende Strukturen aus, etwa über Foundations oder Konsortien. Diese sollen **Richtlinien, Nachweisstandards und Kommunikationsmechanismen** bündeln. Stewards erwarten hier eine **gemeinsame Verantwortung** zwischen Projekten, Industrie und Behörden.

3.6 Kurzüberblick: Vergleichbare, aber anders akzentuierte Themen

Themenbereich (Hersteller)	Entsprechung bei Stewards	Charakter der Aussagen
Einheitliche Standards und Prozesse	Wunsch nach realistischen, vereinfachten Verfahren (Self-Assessment, klare Regeln)	eher pragmatisch als formal
Institutionalisierte Kooperation (Foundations)	Zustimmung, aber Betonung von Freiwilligkeit und Offenheit	vorsichtig, keine Abhängigkeit
Finanzielle Unterstützung der Community	Ja, aber im Sinne nachhaltiger Förderung, nicht Bezahlung pro Nachweis	systemische Finanzierung
Kommunikation & Governance	Betonung auf direkter, vertrauensvoller Zusammenarbeit, insbesondere bei Sicherheitsfragen	weniger formal, mehr pragmatisch
Technische Zusammenarbeit / Tooling	Explizite Forderung nach besseren Werkzeugen und gemeinsamer Infrastruktur	klar formuliert
Rechtliche Klarheit	Erwartung klarer, verständlicher Guidance durch Behörden	explizit mehrfach benannt

Gesamtbewertung: Die Stewards verstehen Kooperation im CRA-Kontext als **gegenseitigen Prozess**, nicht als einseitige Verpflichtung. Sie wünschen sich eine Zusammenarbeit, die auf **Partnerschaft, Transparenz und realistischem Ressourceneinsatz** beruht und damit strukturell nachhaltiger ist als reine Nachweispflichten oder formale Kontrollmechanismen.

3.2.4. Ergebnisse der Befragung der Maintainer von Open Source Projekten

Die Befragung der Open Source Projekte gibt Aufschluss, wie sich die Projekte selbst im Kontext des CRA einordnen und welchen Einfluss der CRA auf die Open Source Community haben könnte.
Die Auswertung der Fragen konzentriert sich auf die folgenden Themenfelder:

- Unklarheiten
- Rolle der Stewards zu Open Source Projekten
- Unterstützungsleistungen

1. Unklarheiten

1.1. Welche Rolle nimmt ein Projekt ein?

57% der Teilnehmenden die die Frage "Wisst ihr, welche Rolle ihr unter dem CRA einnehmen werdet?" explizit beantwortet haben, haben mit Nein geantwortet. Die anderen konnten sagen, dass sie unter dem CRA keine Verpflichtungen haben, ein Steward oder ein Hersteller sind.

1.2. Kommerzieller Hintergrund

Grundsätzliche Unsicherheit besteht nach wie vor um die Eigenschaft der kommerziellen Tätigkeit. Anhand der gegebenen Antworten von OSS-Projekten lässt sich ablesen, dass sich die vielfältigen und sich dynamisch ergebenden Strukturen von Open Source Projekten nicht intuitiv in die Schablone kommerziell/ nicht kommerziell einfügen lassen. Hierbei besteht entsprechende Unsicherheit, ob und welche Akteure des Projekts als Hersteller bzw. als Steward einzustufen sind.

Als zumindest diskutabel wahrgenommene Strukturen waren etwa:

- „OSS-Projekte, die einen einzigen (nennenswerten) Sponsor haben, der die Ergebnisse des Projekts kommerziell nutzt.“
- Die „Organisation mehrerer Akteure um ein OSS-Projekt herum, die kommerzielle Dienstleistungen anbieten, innerhalb eines gemeinnützigen Vereins.“

Ferner bestand die Sorge, dass bestimmte Aktivitäten des Projekts zwar als objektiv kommerziell einzustufen sind, die aber keine substantiellen Finanzierungsmittel mit sich bringen. Dies umfasst etwa den Erlös von Einnahmen durch Spenden, Erlöse in offiziellen App Stores o. Ä., die in ihrer Summe zwar die Realisierung eines Projekts erleichtern, jedoch in Summe nur einen geringen Beitrag zur Aufwandsdeckung des Projekts darstellen. In dieser Kombination besteht entsprechend Unsicherheit, ob eine nicht Deckung der Kosten schlussfolgerlich das Fehlen einer Gewinnerzielungsabsicht darstellt.

Vor diesem Hintergrund sollte ebenfalls erwähnt werden, dass der Großteil der Befragten OSS-Projekte angab, dass zu erwartende Spenden die Kosten zur Betreuung des Projekts nicht decken.

- „Gibt es eventuell eine Geringfügigkeitsgrenze bezüglich der Monetarisierung des Projektes, deren Unterschreiten es uns ermöglichen würde, rechtlich nicht als Hersteller, sondern als Maintainer/Entwickler angesehen werden und wie hoch ist diese in EUR/Jahr?“
- „Ab welchen Schritten der Kommerzialisierung muss ich Maßnahmen nach dem CRA ergreifen?“
- „Wenn es nur einen einzigen Sponsor gibt, ist es dann kommerziell?“
- „Wir sind sehr unsicher, ab wo genau sich ein "kommerzieller Hintergrund" ergeben würde. Es gibt kommerzielle Anbieter rund um das Produkt, Schulung, Hosting, Weiterentwicklung. Die sind auch als Mitglieder (neben anderen) in einem gemeinnützigen e.V. organisiert. Auch die Gemeinnützigkeit des Vereins steht bisweilen in Frage, wir vermuten, dass bezüglich CRA die gleichen Probleme/Fragen auf uns zukommen könnten.“
- „I don't understand responsibilities and legal liability relative to where commercialisation is taking place. For example, if commercial activities are under a separate legal entity, but the project itself remains under my personal control & maintainership, am I personally liable due to commercialisation of a technically separate legal entity?“
- „I am making money from Open Source development. This probably makes me a manufacturer. I can not fulfill the roles of a manufacturer unless I get paid a lot more money, but it is unlikely that anybody will do that. So it is unclear how I can keep my marginal business afloat.“

1.3. Pflicht zur Erfüllung der CRA-Anforderungen

Unsicherheit und Befürchtungen gibt es auch, ob die Anforderungen des CRA von den Open Source Projekten erfüllt werden müssen. Analog zu den Fragen bezüglich der Rollen und des kommerziellen Hintergrunds unter dem CRA zeigt sich auch hier, dass dementsprechend nicht immer klar ist, ob die Anforderungen erfüllt werden müssen.

- „Unklarheit in der rechtlichen Praxis“
- „Fear of breaking the law because of complexity and unclear requirements“

Hinzu kommt die Befürchtung, dass von einigen Herstellern, die eine Open Source Komponente in ihre Produkte integrieren, Druck aufgebaut wird, obwohl das entsprechende Open Source Projekt gar nicht unter den CRA fällt.

- „Indirekt dadurch, dass die OSS in kommerziellen Produkten genutzt wird. Hierdurch kann seitens der kommerziellen Nutzer Druck auf das OSS-Projekt entstehen."
- „Auf der einen Seite die Unsicherheit bezüglich der kommerziellen Tätigkeit. Wir nehmen an, dass wir im Zweifel nicht wissen, ob wir Steward oder Manufacturer sind, bis wir von einer Marktaufsicht auf eines der beiden gecalled werden. Außerdem nehmen wir an, dass es Anspruchsinhaber geben könnte, aus der Community oder bei den Kunden, die verlangen, dass wir die Manufacturer-Anforderungen erfüllen, egal ob wir müssten oder nicht."
- „Compliance-Anforderungen von Business-Nutzern"

Es gibt aber auch Open Source Projekte, die für sich ganz klar feststellen, dass sie nicht unter die Verpflichtungen des CRA fallen und dementsprechend keine Anforderungen erfüllen müssen.

- „Nein, ich war mehrfach auf der FOSDEM Konferenz und habe Vorträge zum CRA gehört. Nach meinem besten Wissen bin ich von keiner Anforderung des CRA betroffen."

1.4. CRA-Kennzeichnung von Projekten

Die Mehrheit wünscht sich eine Art Kennzeichnung in ihren Projekten, dass sie nicht unter den CRA fallen, um den Nutzenden zu zeigen, dass sie keine Verpflichtungen erfüllen.

2. Mögliche Rolle der Stewards aus Sicht der Projekte

Die Mehrheit der befragten Open Source Projekte kann sich nicht vorstellen, dass jemand für sie die Rolle des Stewards übernimmt. Stattdessen wollen sie selbst Steward für ihr Projekt werden, falls es sich für sie aufdrängt. Die Problematik der Wahrnehmung von Stewards zeigt sich in folgenden Zitaten:

- „Wir würden keinen externen Steward akzeptieren um Kontrollverlust zu vermeiden; außerdem ist fraglich, warum jemand externes diese Dienstleistung übernehmen sollte, ohne dass monetäre Motivation dahintersteckt - was wiederum für uns zum Problem würde, weil das Entwickeln des Produkts eben gerade NICHT hauptsächlich monetär motiviert war. Da besteht ein Zielkonflikt."
- Hinzu: „Die sind auch als Mitglieder (neben anderen) in einem gemeinnützigen e.V. organisiert. Auch die Gemeinnützigkeit des Vereins steht bisweilen in Frage, wir vermuten, dass bezüglich CRA die gleichen Probleme/Fragen auf uns zukommen könnten".
    - ➢ Als mögliches Problem oder möglicher Konflikt wird die Frage wahrgenommen, inwieweit z.B. Vereine Stewards werden, aber Stewards als „monetär motiviert" wahrgenommen werden.

3. Unterstützungsleistungen

3.1. Unterstützung für eine mögliche freiwillige Erfüllung der Anforderungen

Es gibt Open Source Projekte, die sich vorstellen können, die „Allgemeinen Anforderungen“ des CRA zu erfüllen. Dazu wird in den Interviews darauf hingewiesen, dass konkrete Umsetzungshinweise, Tools und Funding benötigt werden.

- „Möglichst breite FAQs und rechtliche Beratung“
- „Eine Checkliste der Anforderungen mit Erläuterungen“
- „Clear checklists and funding for additional efforts.“
- „Tooling for generating SBOMs automatically, preferably very easy to integrate in CI pipelines“

Es gibt aber auch Open Source Projekte, die für sich erklären, dass sie die Anforderungen nicht erfüllen müssen und entsprechend keine Unterstützung dahingehend benötigen.

- „Keine - würde der CRA zu bedeutender Mehrarbeit führen, würde ich die Projekte von GitHub löschen!”
- „I see no reason to.”

3.2. Langfristige Förderung von OSS-Projekten im Bereich Wissenschaft

Als eine erhebliche Schwierigkeit hinsichtlich eines langfristig CRA konformen Einsatzes von Open Source Komponenten wird das „Verwaisen“ von Projekten angesehen. Im Rahmen der Umfrage wurde von mehreren OSS-Projekten angemerkt, dass dies umso wahrscheinlicher ist, sofern ein OSS-Projekt im Wesentlichen von (ggf. öffentlichen) Förderstrukturen abhängt. So ist es im wissenschaftlichen Bereich etwa gängig, im Rahmen eines durch Drittmittel geförderten Forschungsprojekts Softwarekomponenten als Open Source verfügbar zu machen. Die Struktur der Projektbeitragenden verdient somit nicht direkt (etwa durch Spenden) Geld mit dem Projekt, jedoch geschieht ihre Arbeit nicht allein aus altruistischen Motiven. Entsprechend groß ist die Gefahr, dass ein OSS-Projekt, gerade im wissenschaftlichen Bereich verwaist, sobald ein gefördertes Projekt fertiggestellt und kein fachlich nahes Anschlussprojekt bewilligt wird. Der Lebenszyklus solcher Projekte ist entsprechend stark an die Förderzyklen (und Trends) im Bereich der Forschungsdrittmittel gebunden. Werden derartige Projekte in CRA relevanten Produkten eingesetzt, ist es wichtig, ein nachhaltiges Maintaining und damit auch eine Finanzierung sicherzustellen.

3.2.5. Unterstützungsleistungen

Alle Stakeholdergruppen sprechen sich dafür aus, dass einfache und verständliche Regelungen vorliegen, die im optimalen Falle auch durch Tools abgebildet werden können. Zudem haben vor allem Projekte und potentielle Stewards immer wieder auf Finanzierungsprobleme hingewiesen, die durch die jetzigen Unterstützungen, etwa durch Spenden, nicht ausreichend abgedeckt werden.
Unklar bleibt, wie etwa finanzielle Unterstützungsleistungen von wem, für was, wie, in welchem Umfang zur Verfügung gestellt werden sollen.

4. Fazit

Übergreifend lässt sich festhalten, dass die Befragten vor allem den Wunsch nach Klarheiten in Hinblick auf die unterschiedlichen Rollen und ihrer konkreten Ausgestaltung bestätigen. Vor allem die Frage ab wann man in welche Rolle fällt bedarf einer konkreten Ausformulierung. Hierfür kann die von der EU-Kommission angestoßene Guidance eine Lösung sein.

Ebenfalls übergreifend äußerten die Befragten den Wunsch nach Tools, die ihnen in den jeweiligen CRA Workflows helfen, die entsprechenden Vorgaben zu erfüllen.

Zudem fragen sich vor allem potentielle Stewards, wie sie mit möglichen Kosten, die auf sie zukommen, umgehen sollen. Diese Frage entwickelt vor allem für die Hersteller, die keine Verbindungen zu eben jenen Projekten haben ebenfalls eine Relevanz, da Hersteller tendenziell Projekte nicht forken wollen. Daher muss ein Modus gefunden werden, in dem Gelder und/oder nötige Ressourcen für die potentielle Stewards zur Verfügung gestellt werden. In diesem Zusammenhang stellt sich auch die Frage, wie mit der zeitlichen Dimension von CVE Fixes umzugehen ist, ohne Projekte zu überfordern und wie mit Projekten umzugehen ist, die nicht mehr maintained werden.

Eine weitere Fragestellung hat sich zudem in Hinblick auf Artikel 25 und die Attestierung von Komponenten ergeben. Dieses Problemfeld wurde in dem vorliegenden Fragebogen nur am Rande adressiert, wird aber in den folgenden Monaten eine entscheidende Rolle spielen. Die bisherigen Antworten im Fragebogen legen nahe, sich dezidiert mit dem Problemfeld auseinanderzusetzen, da hier ebenfalls viele Unklarheiten vorherrschen. So stellt sich etwa die Frage, von wem wie eine Attestierung durchgeführt werden kann und wie diese finanziert wird.

Die Diskussionen sowie die Auswertung der Umfrageergebnisse legen nahe, dass ein strukturierter Austausch zwischen den verschiedenen Stakeholdern notwendig ist. Nur durch einen gemeinsamen Dialog können Anforderungen und Erwartungen aller Seiten

berücksichtigt und ein konsensfähiger Ansatz für die zukünftige Zusammenarbeit entwickelt werden. Andernfalls droht die Gefahr, dass isoliert erarbeitete Lösungen auf Unverständnis oder Ablehnung bei anderen Beteiligten stoßen.

Die Ergebnisse des Workstreams, insbesondere der Befragung, werden im weiteren Vorgehen der EU-Kommission und den Marktüberwachungen zur Verfügung gestellt, um sicherzustellen, dass die aufgeworfenen Fragen und Problemfelder im weiteren Prozess adressiert werden.

5. Anlage: Fragebögen und Auswertung

Zum besseren Verständnis der Umfrage sowie der Ermutigung mit den Ergebnissen weiter zu arbeiten, sind nun alle Rohdaten und Ergebnisse hier zu finden: https://cooperation.dialog-cybersicherheit.de/s/pJ7HgySKMS6H3Kg.

Fragebögen und Auswertung in der Reihenfolge: Hersteller & Manufacturer (DE & EN), Stewards (DE & EN) und OSS-Projekte (DE & EN).

Fragebogen für Hersteller in Bezug auf den CRA

Ergebnisse

Umfrage 552671

Anzahl der Datensätze in dieser Abfrage:	66
Gesamtzahl der Datensätze dieser Umfrage:	66
Anteil in Prozent:	100.00%

Zusammenfassung für Q00

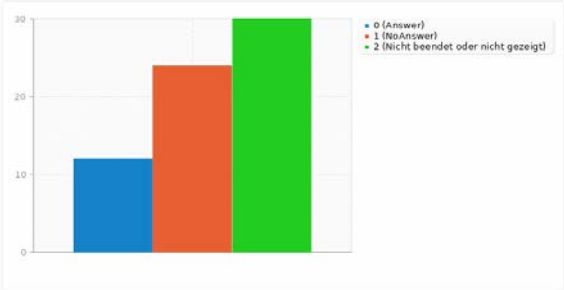
Welche Risiken seht ihr beim Einsatz von Open-Source-Komponenten in euren Produkten?(Sicherheitsrisiken / organisatorische Risiken)

Antwort	Anzahl	Prozent
Antwort	12	18.18%
Keine Antwort	24	36.36%
Nicht beendet oder nicht gezeigt	30	45.45%

ID	Antwort
136	Hauptrisiko ist, dass die Komponenten nicht mehr angemessen gepflegt und weiter entwickelt werden, dass sie dadurch unsicher werden und dass wir die zur eigenständigen Pflege notwendige Kompetenz nicht schnell genug aufbauen oder einkaufen können.
137	Zentrales Risiko ist immer, dass eine OSS-Komponente nicht mehr in angemessener Form weiterentwickelt oder sicher gehalten wird.
145	Supply-chain-Attacks, Lizenz-Probleme, schlechte Qualität/langsames Bug- oder CVE-Fixing
163	Sicherheitsrisiken: fehlendes Management von CVEs; ungenügende Updatezyklen organisatorisch: Komplexität der Handhabung steigt
167	Malware in den Sourcen, Dependency Confusion Angriffe , Nicht zur Verfügung stehende Open Source, Lizenzrechtlich und arbeitsrechtlich saubereres Patchen,
174	Sicherheitsrisiken: Versuche, Schadcode in "wichtige" Repos einzuschleusen, fehlende oder mangelhafte Sicherheit (unsicheres Design) Organisatorisches Risiko: End Of Life / Abandonment, Nachweis der Sicherheit (insbesondere bei großen / komplexen Komponenten), ungeeignete Lizenzen
175	Lizenz-Risiken, Sicherheits-Risiken, organisatorische Risiken (z.B. die Community löst sich auf)
177	Langzeitverfügbarkeit von Updates und Wartung, Lizenzänderung während der Nutzungsdauer und evtl. keine Möglichkeit mehr zur Nutzung von Updates
178	Die nicht-lizenzkonforme Nutzung von OSS durch Lieferanten und dadurch das Fehlen sämtlicher durch den CRA geforderten Due-Dilligence für eben diese Bestandteile.
179	Grundsätzlich die Selben wie bei kommerzieller Software. Supply Chain Angriffe sind leicht anders zu bewerten. Die Compliance-Fragen der CRA erhöhen das Risiko.
186	Die klassischen Risiken in der SBOM. Insgesamt ist OpenSource transparenter als CloseSource, Risiken sind besser mitigierbar.
197	Mangelhafte Pflege durch das Projekt, fehlende Ansprechbarkeit

Zusammenfassung für Q00

Welche Risiken seht ihr beim Einsatz von Open-Source-Komponenten in euren Produkten?(Sicherheitsrisiken / organisatorische Risiken)



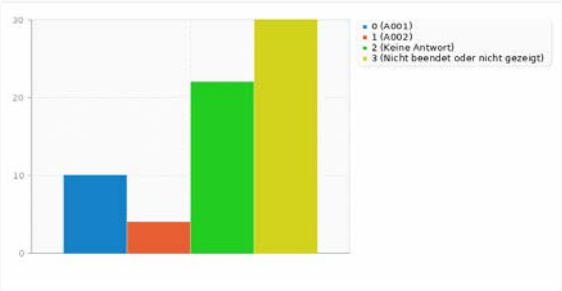
Zusammenfassung für Q001

Führt ihr bereits eine Due-Diligence-Prüfung und Risikobewertung für Ihre Open-Source-Komponenten durch?

Antwort	Anzahl	Prozent
ja (A001)	10	15.15%
nein (A002)	4	6.06%
Keine Antwort	22	33.33%
Nicht beendet oder nicht gezeigt	30	45.45%

Zusammenfassung für Q001

Führt ihr bereits eine Due-Diligence-Prüfung und Risikobewertung für Ihre Open-Source-Komponenten durch?



Zusammenfassung für Q002

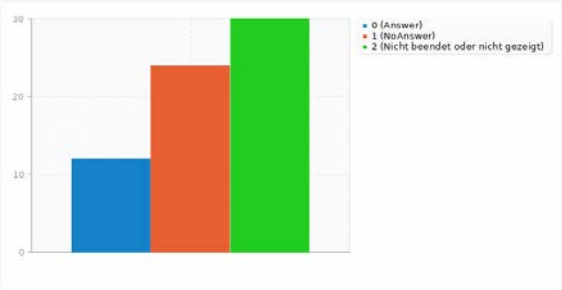
Habt ihr einen Notfallplan (welchen?) für den Fall, dass einige der kritischen Open-Source-Projekte, auf die ihr euch verlasst, von den Entwicklern aufgegeben werden?

Antwort	Anzahl	Prozent
Antwort	12	18.18%
Keine Antwort	24	36.36%
Nicht beendet oder nicht gezeigt	30	45.45%

ID	Antwort
136	Keinen fertigen Plan, aber wir monitoren die Situation kontinuierlich, versuchen Kontakt in relevante Communities aufzubauen und zeitnah Lösungen zu finden.
137	Wir haben eine Vorstellung und Liste möglicher Handlungsoptionen, aber keinen fertigen Plan.
145	ja, (-> interne Information)
163	ja
167	Nein, noch nicht implementiert
174	Wir würden für unsere kritischen Komponenten vergleichbare Alternativen wählen. Bei den meisten ist dies aber sehr unwahrscheinlich, weil sie zu weit verbreitet sind. Notfalls können wir die Projekte auch für eigene Zwecke selbst weiter pflegen, jedenfalls für eine Übergangszeit.
175	Es gibt verschiedene Mitigationsmöglichkeiten: Z.B.: Das Projekt forken und selbst warten bzw. weiterentwickeln, auf ein anderes Projekt, das eine ähnliche Funktionalität anbietet, umsteigen, rechtzeitig Contributors aus dem eigenen Unternehmen aufbauen.
177	Einsatz von Alternativen, Änderung Systemarchitektur oder Produkt sofort abkündigen
178	Nicht für alle, aber für einige Komponenten gibt es eine "Second Source". Für die von den Entwicklern aufgegebene OSS haben wir ja durch die OSS-Lizenz(en) eine uneingeschränkte Nutzung, die auch eine Veränderung, also die Wartung und ggf. eigenständige Beseitigung von Sicherheitsproblemen umfasst. Der Austausch einer Komponente oder die eigenständige Pflege ist immer eine Kosten-Nutzen-Frage.
179	Grundsätzlich schon. Eigene Wartung, Information über Alternativen. Das Risiko ist vgl. zu kommerziellen Produkten.
186	nein
197	Ja - schlimmstenfalls Pflege selbst übernehmen. Besser gemeinsam mit anderen eine Lösung finden, z.B. im Rahmen des Debian-Projektes.

Zusammenfassung für Q002

Habt ihr einen Notfallplan (welchen?) für den Fall, dass einige der kritischen Open-Source-Projekte, auf die ihr euch verlasst, von den Entwicklern aufgegeben werden?



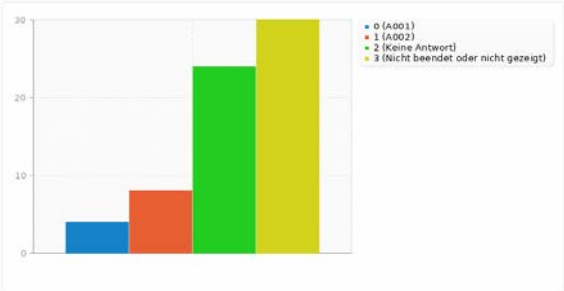
Zusammenfassung für Q003

Plant ihr Open Source Projekte wegen dem CRA zu forken/selber pflegen?

Antwort	Anzahl	Prozent
ja (A001)	4	6.06%
nein (A002)	8	12.12%
Keine Antwort	24	36.36%
Nicht beendet oder nicht gezeigt	30	45.45%

Zusammenfassung für Q003

Plant ihr Open Source Projekte wegen dem CRA zu forken/selber pflegen?



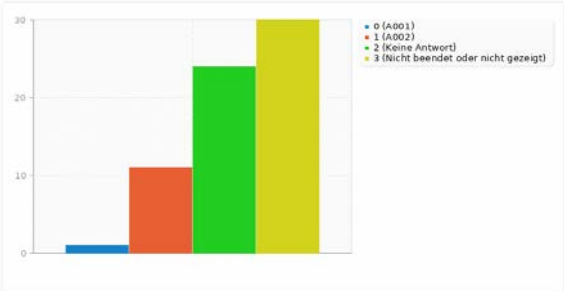
Zusammenfassung für Q004

Plant ihr Open Source Projekte wegen dem CRA durch proprietäre Software zu ersetzen?

Antwort	Anzahl	Prozent
ja (A001)	1	1.52%
nein (A002)	11	16.67%
Keine Antwort	24	36.36%
Nicht beendet oder nicht gezeigt	30	45.45%

Zusammenfassung für Q004

Plant ihr Open Source Projekte wegen dem CRA durch proprietäre Software zu ersetzen?



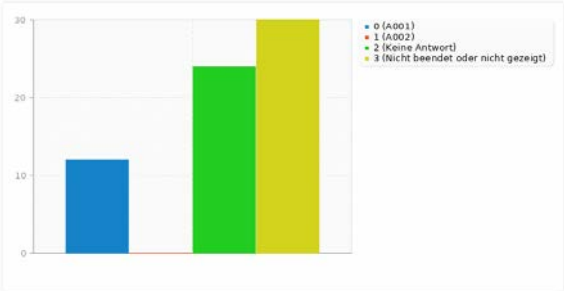
Zusammenfassung für Q005

Verfügen Sie über einen Prozess für das Schwachstellenmanagement Ihrer Produkte, der auch Open-Source-Abhängigkeiten abdeckt, um mit der CRA konform zu sein?

Antwort	Anzahl	Prozent
ja (A001)	12	18.18%
nein (A002)	0	0.00%
Keine Antwort	24	36.36%
Nicht beendet oder nicht gezeigt	30	45.45%

Zusammenfassung für Q005

Verfügen Sie über einen Prozess für das Schwachstellenmanagement Ihrer Produkte, der auch Open-Source-Abhängigkeiten abdeckt, um mit der CRA konform zu sein?



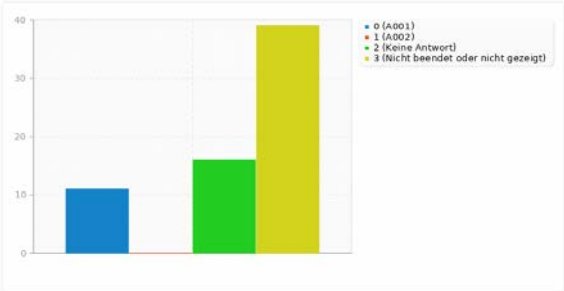
Zusammenfassung für Q006

Befolgt ihr bereits Vorschriften oder Standards in Bezug auf Cybersecurity?

Antwort	Anzahl	Prozent
ja (A001)	11	16.67%
nein (A002)	0	0.00%
Keine Antwort	16	24.24%
Nicht beendet oder nicht gezeigt	39	59.09%

Zusammenfassung für Q006

Befolgt ihr bereits Vorschriften oder Standards in Bezug auf Cybersecurity?



Zusammenfassung für Q007

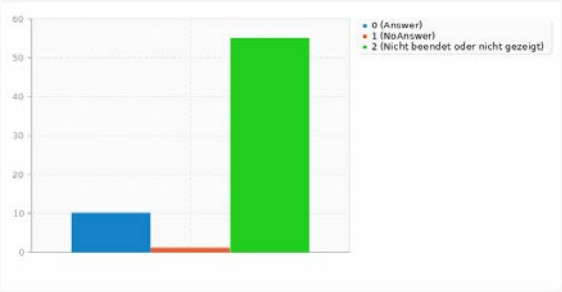
Welche Verordnungen oder Standards sind das?

Antwort	Anzahl	Prozent
Antwort	10	15.15%
Keine Antwort	1	1.52%
Nicht beendet oder nicht gezeigt	55	83.33%

ID	Antwort
136	It Grundschutz
137	BSI Grundschutz
163	SBOM, CVE-Management, Risikobewertung usw.
167	IEC 62443; IEC 29147, IEC 30111, Prozesse noch unvollständig implementiert, Gerade im Aufbau
174	ISO 27001, (NIS-2 so weit es geht), KI-Verordnung, DSGVO
177	IEC 62443-4-1
178	ISO 31000 ISO/IEC 27001 ISO/IEC 27701 ISO 22301 ISO/IEC 15408 ISO/IEC 30111 ISO/IEC 29147 IEC 62443 ISO/SAE 21434 ISO 24089 IEC 63452 ...
179	ISO27001
186	Nicht um des Standarts willen sondern um Sicherheit zu erhöhen.
197	BSI Grundschutz

Zusammenfassung für Q007

Welche Verordnungen oder Standards sind das?



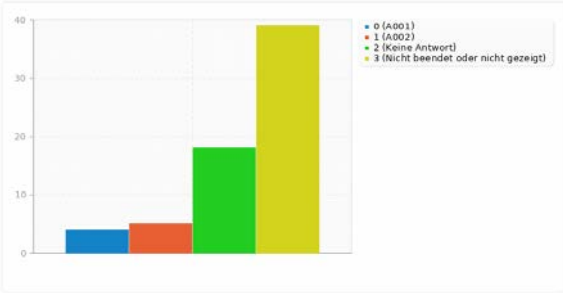
Zusammenfassung für Q008

Kann für die eingebunden Open Source Komponenten aus eigenen Mitteln sichergestellt werden, dass die Anforderungen des CRA erfüllt werden?

Antwort	Anzahl	Prozent
ja (A001)	4	6.06%
nein (A002)	5	7.58%
Keine Antwort	18	27.27%
Nicht beendet oder nicht gezeigt	39	59.09%

Zusammenfassung für Q008

Kann für die eingebunden Open Source Komponenten aus eigenen Mitteln sichergestellt werden, dass die Anforderungen des CRA erfüllt werden?



Zusammenfassung für Q009

Wie geht ihr mit Open Source Komponenten um, von denen ihr nicht wisst, ob sie die Anforderungen des CRA erfüllen?

Antwort	Anzahl	Prozent
Wir ignorieren das Projekt (A001)	1	1.52%
Wir kontaktieren das Projekt / die Entwickler (A002)	5	7.58%
Wir helfen dem Projekt (A003)	2	3.03%
Keine Antwort	19	28.79%
Nicht beendet oder nicht gezeigt	39	59.09%

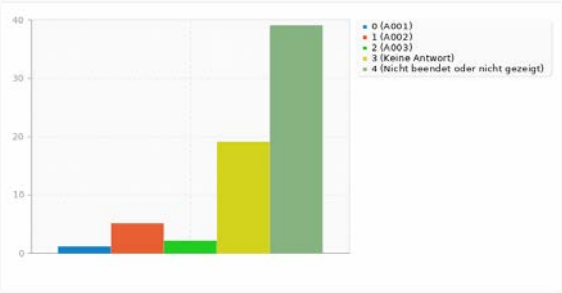
Zusammenfassung für Q010

Seht ihr Anforderungen des CRA für die es schwierig ist sicherzustellen, dass die im Produkt integrierten Open Source Komponenten diese erfüllen?

Antwort	Anzahl	Prozent
ja (A001)	5	7.58%
nein (A002)	1	1.52%
Keine Antwort	21	31.82%
Nicht beendet oder nicht gezeigt	39	59.09%

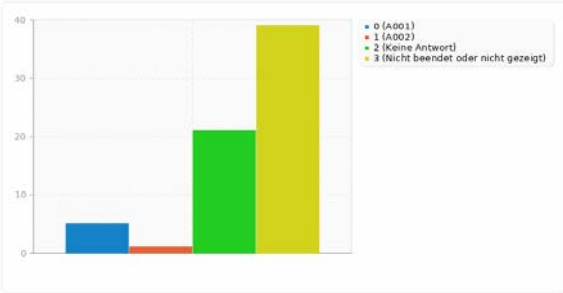
Zusammenfassung für Q009

Wie geht ihr mit Open Source Komponenten um, von denen ihr nicht wisst, ob sie die Anforderungen des CRA erfüllen?



Zusammenfassung für Q010

Seht ihr Anforderungen des CRA für die es schwierig ist sicherzustellen, dass die im Produkt integrierten Open Source Komponenten diese erfüllen?



Zusammenfassung für Q011

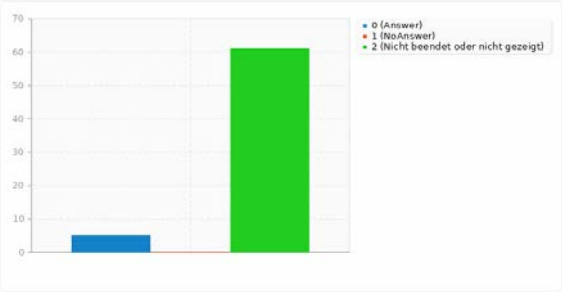
Welche sind das und und warum ist es schwierig?

Antwort	Anzahl	Prozent
Antwort	5	7.58%
Keine Antwort	0	0.00%
Nicht beendet oder nicht gezeigt	61	92.42%

ID	Antwort
167	Wo wird ein CE Zeichen angebracht? Wie ist das nachweisbar dass es kein Fake ist? viele Projekte sind ausserhalb der EU und legen noch keinen Wert auf Sicherheit.
174	Wir nutzen viele open source-Komponenten. Für alle die Erfüllung von Anhang I sicherzustellen ist eine vollkommen weltfremde Vorstellung; der Aufwand wäre absurd hoch - zumal wir die Projekte allesamt von Grund auf aufarbeiten müssten. Ein Nachweis für ein einzelnes Projekt wäre ggf. möglich. Der Nachweis müsste von den open source-Herstellern oder durch vollständig automatisiertes Tooling (ausnahmslos (!) kein manueller Aufwand) erbracht werden.
177	Security Support Period von 10 bis 15 Jahren
178	Es wird eine Zweiklassengesellschaft im Open Source etabliert: Die, die von sich aus den CRA "befolgen" und z.B. einen OSS-Steward haben und eine Vielzahl von Projekten, die es nicht können oder, weil eben nicht-EU-dominiert, sich nicht darum scheren.
197	Von Freiwilligen verfolgte Projekte können kein Commitment zur langfristigen Pflege aufbringen.

Zusammenfassung für Q011

Welche sind das und und warum ist es schwierig?



Zusammenfassung für Q012

Wisst ihr, wer die Open Source Komponenten, die ihr in euren Produkten einsetzt, entwickelt?

Antwort	Anzahl	Prozent
ja (A001)	9	13.64%
nein (A002)	2	3.03%
Keine Antwort	10	15.15%
Nicht beendet oder nicht gezeigt	45	68.18%

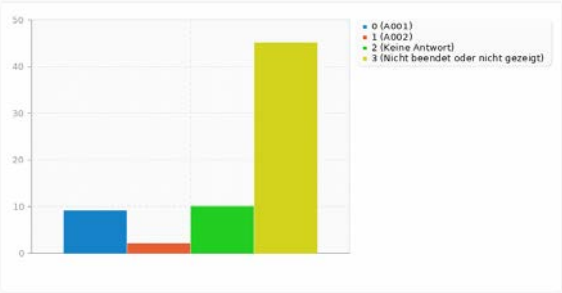
Zusammenfassung für Q013

Arbeitet ihr mit den euch bekannten Anbietern der Open Source Komponenten zusammen?

Antwort	Anzahl	Prozent
ja (A001)	7	10.61%
nein (A002)	4	6.06%
Keine Antwort	10	15.15%
Nicht beendet oder nicht gezeigt	45	68.18%

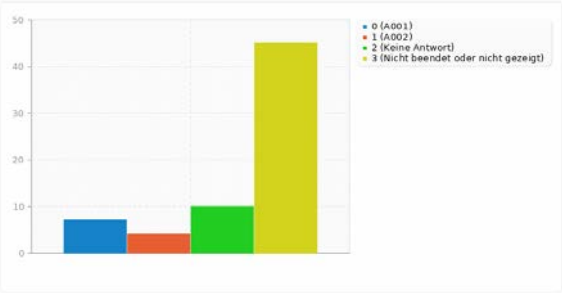
Zusammenfassung für Q012

Wisst ihr, wer die Open Source Komponenten, die ihr in euren Produkten einsetzt, entwickelt?



Zusammenfassung für Q013

Arbeitet ihr mit den euch bekannten Anbietern der Open Source Komponenten zusammen?



Zusammenfassung für Q014

Würde ein Nachweis helfen, dass Open Source Komponenten die CRA Anforderungen erfüllen.

Antwort	Anzahl	Prozent
ja (A001)	11	16.67%
nein (A002)	1	1.52%
Keine Antwort	9	13.64%
Nicht beendet oder nicht gezeigt	45	68.18%

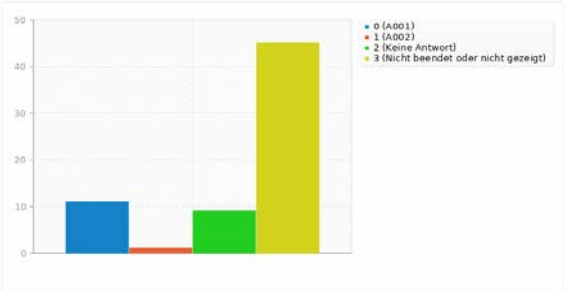
Zusammenfassung für Q015

Für den Fall, dass es einen Nachweis für die Erfüllung der CRA Anforderungen für Open Source Komponenten gibt: Ist die Bereitschaft da, für diese zu bezahlen?

Antwort	Anzahl	Prozent
ja (A001)	7	10.61%
nein (A002)	1	1.52%
Keine Antwort	13	19.70%
Nicht beendet oder nicht gezeigt	45	68.18%

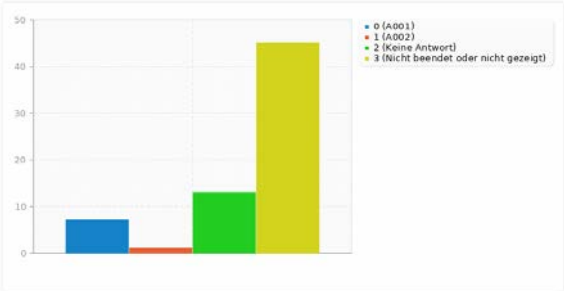
Zusammenfassung für Q014

Würde ein Nachweis helfen, dass Open Source Komponenten die CRA Anforderungen erfüllen.



Zusammenfassung für Q015

Für den Fall, dass es einen Nachweis für die Erfüllung der CRA Anforderungen für Open Source Komponenten gibt: Ist die Bereitschaft da, für diese zu bezahlen?



Zusammenfassung für Q016

Arbeitet ihr jetzt schon mit potentiellen Stewards zusammen?

Antwort	Anzahl	Prozent
ja (A001)	3	4.55%
nein (A002)	6	9.09%
Keine Antwort	11	16.67%
Nicht beendet oder nicht gezeigt	46	69.70%

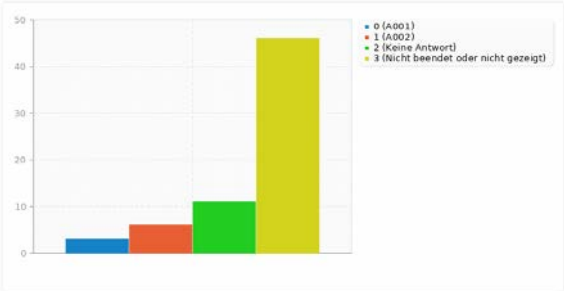
Zusammenfassung für Q017

Unterstützt ihr diese, bzw. plant ihr diese zu unterstützen?

Antwort	Anzahl	Prozent
ja (A001)	3	4.55%
nein (A002)	3	4.55%
Keine Antwort	14	21.21%
Nicht beendet oder nicht gezeigt	46	69.70%

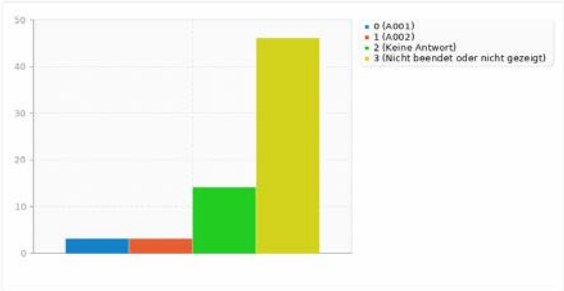
Zusammenfassung für Q016

Arbeitet ihr jetzt schon mit potentiellen Stewards zusammen?



Zusammenfassung für Q017

Unterstützt ihr diese, bzw. plant ihr diese zu unterstützen?



Zusammenfassung für Q018

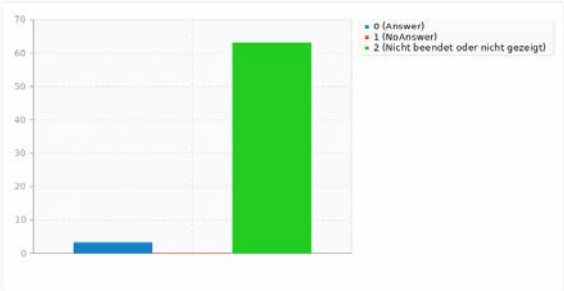
Wie sieht diese Unterstützung aus?

Antwort	Anzahl	Prozent
Antwort	3	4.55%
Keine Antwort	0	0.00%
Nicht beendet oder nicht gezeigt	63	95.45%

ID	Antwort
175	Beitragen, monetäre Unterstützung
178	- Beträge an eine Foundation, die die Mittel für die Stewards verwendet. - Mitarbeit bei der Erarbeitung von Methoden und Prozessen, die vom Steward umgesetzt werden sollen - Überprüfung ob wir selbst Stewards stellen sollen und wie die Kompetenz aufgebaut werden kann
197	Finanzielle Unterstützung, Sponsoring, Mitarbeit.

Zusammenfassung für Q018

Wie sieht diese Unterstützung aus?



Zusammenfassung für Q019

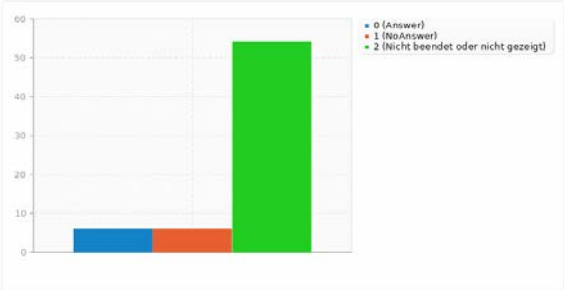
Welche Unterstützung, und vom wem, wird benötigt, um sicherzustellen, dass Open Source Komponenten in ihren Produkten die CRA Anforderungen erfüllen?

Antwort	Anzahl	Prozent
Antwort	6	9.09%
Keine Antwort	6	9.09%
Nicht beendet oder nicht gezeigt	54	81.82%

ID	Antwort
137	Für Projekte sollte es einen sehr einfachen Weg geben, das Einhalten der Anforderungen nachweisbar zu machen und für solche Nachweise auch in angemessener Weise vergütet zu werden.
174	Es muss eine Stelle oder ein Tool geben, welche die Sicherheit von open source-Komponenten CRA-konform sicherstellt. Die Kosten müssen angesichts der Menge der verwendeten Komponenten sehr überschaubar sein. Hersteller sollten da außen vor sein.
175	Soweit wir den CRA verstanden haben, fallen Open-Source-Projekte nicht unter die CRA-Regeln. Insofern macht die Frage keinen Sinn. Am Ende müssen die Produkte die CRA-Anforderungen erfüllen.
178	1) die Community sollte sich abgestimmten Regeln unterwerfen 2) ein Mechanismus, der eine positive CRA-Bewertung durch Dritte auch wieder an die Community zurückspielt
179	Eigtl. ist doch im CRA nicht-kommerzielle Software ausgenommen. Wenn wir diese als Grundlage für eigene Software nutzen, sahen wir bisher hier keinen Handlungsbedarf. Eine Unterstützung für rechtliche Beratung wäre wirklich sehr wichtig.
197	Ein Mix - Übernahme kritischer Kernkomponenten ohne Pflege durch Stewards oder andere Organisationen, Sponsoring und Förderung, Infrastruktur die dazu führt, das Konsumenten von OSS auch für deren Sicherheit und Pflege zahlen.

Zusammenfassung für Q019

Welche Unterstützung, und vom wem, wird benötigt, um sicherzustellen, dass Open Source Komponenten in ihren Produkten die CRA Anforderungen erfüllen?



Zusammenfassung für Q020

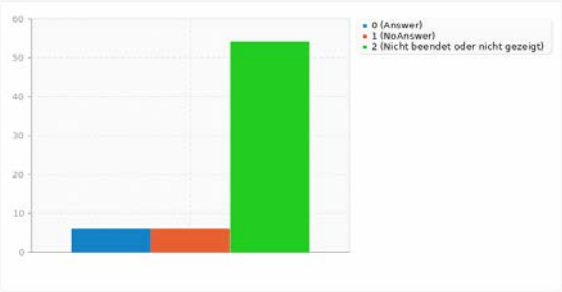
Wie kann aus Herstellersicht eine Zusammenarbeit mit Open Source aussehen (speziell mit den Stewards)?

Antwort	Anzahl	Prozent
Antwort	6	9.09%
Keine Antwort	6	9.09%
Nicht beendet oder nicht gezeigt	54	81.82%

ID	Antwort
137	Idealerweise zahlen Hersteller, die die Erfüllung der CRA Anforderungen einer Komponente nicht selber sicher stellen wollen, dafür über eine Plattform eine Beitrag, der den Projekten zu Gute kommt. Im Gegenzug sichern Projekte (direkt oder über Stewards) die Einhaltung der CRA Anforderungen zu.
163	bspw. über Gremien wie die Eclipse Foundation o.ä.
174	Die Stewards stellen einen Nachweis der CRA-Erfüllung zur Verfügung, den wir automatisiert verarbeiten.
175	Stewards können/sollten ihre Projekt attraktiver für kommerzielle Verwender machen, indem sie die CRA-Regeln einhalten (auch wenn sie das rein rechtlich nach unserer Information nicht müssten).
178	OSS Community bittet Hersteller um eine Bereitstellung der Zertifizierungen, die für die Inverkehrbringung des Produktes benötigt werden. Auch ein "Outsourcing" von Qualifizierungsmaßnahmen an Hersteller von der Community könnte denkbar sein.
197	Hersteller sollten grundsätzlich die Freiheit haben, die Sicherheit von OSS Komponenten entweder selbst herzustellen oder mit Stewards oder anderen Organisationen zusammen arbeiten, so lange sie nachweisen können, dass sie es ordentlich machen. Wenn sie sich für Stewards entscheiden können hier Vereinbarungen über die Nutzung von Zertifikaten für sichere Komponenten ausgestellt und bezahlt werden.

Zusammenfassung für Q020

Wie kann aus Herstellersicht eine Zusammenarbeit mit Open Source aussehen (speziell mit den Stewards)?



Zusammenfassung für Q021

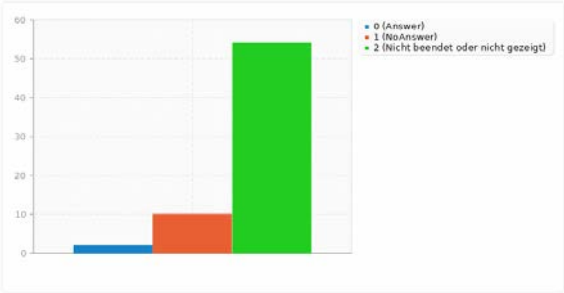
Welche Vereinbarungen sollten getroffen werden?

Antwort	Anzahl	Prozent
Antwort	2	3.03%
Keine Antwort	10	15.15%
Nicht beendet oder nicht gezeigt	54	81.82%

ID	Antwort
174	Der Nachweis ist jederzeit aktuell zu halten, und kann nur mit Vorlaufzeit von ca. 2 Jahren eingestellt werden.
197	s.o.: Steward kann sicherstellen, dass Komponente sicher ist und das zertifizieren. Nutzung des Zertifikates kann kostenpflichtig sein.

Zusammenfassung für Q021

Welche Vereinbarungen sollten getroffen werden?



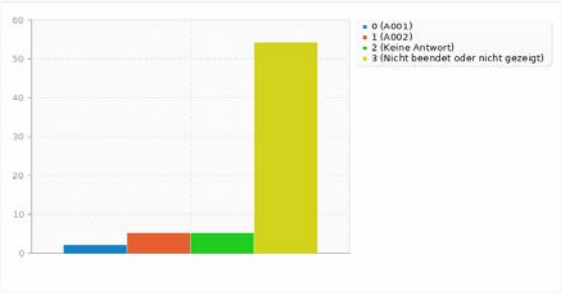
Zusammenfassung für Q022

Wird aus Herstellersicht eine rechtliche Beratung für die Zusammenarbeit mit Stewards / Open Source Projekten benötigt?

Antwort	Anzahl	Prozent
ja (A001)	2	3.03%
nein (A002)	5	7.58%
Keine Antwort	5	7.58%
Nicht beendet oder nicht gezeigt	54	81.82%

Zusammenfassung für Q022

Wird aus Herstellersicht eine rechtliche Beratung für die Zusammenarbeit mit Stewards / Open Source Projekten benötigt?



Questionnaire for Manufacturers in terms of CRA

Ergebnisse

Umfrage 582853

Anzahl der Datensätze in dieser Abfrage:	38
Gesamtzahl der Datensätze dieser Umfrage:	38
Anteil in Prozent:	100.00%

Zusammenfassung für Q00

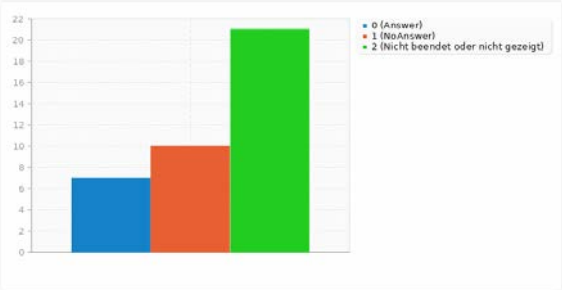
What risks do you see when using open source components in your products (security risks / business risks / other risks)?

Antwort	Anzahl	Prozent
Antwort	7	18.42%
Keine Antwort	10	26.32%
Nicht beendet oder nicht gezeigt	21	55.26%

ID	Antwort
39	None in particular that are specific to open source
49	Incorporating software with security vulnerabilities creating product vulnerabilities, exposing proprietary IP/Code to disclosure obligations, violating open source licenses and exposing company to infringement risk
52	In no particular order: - Exhaustion of patented IPR. - Having to release code under an OSS license, not destined for release. - Liability resulting from lack of knowledge of implementation (normally addressed by indemnification by suppliers). - Providing insight in weaknesses in respect of unknown zero-days. - Providing access to the platform to malicious parties - think trojans in resold products.
57	upstream maintenance is unreliable and cannot get security fixes or features upstream - not having enough capacity to take over maintainership to address needs for customers
64	Security risks due to requirement to quickly respond to new vulnerabilities
69	License risk, EOL and cVe
72	EoL, Security risk

Zusammenfassung für Q00

What risks do you see when using open source components in your products (security risks / business risks / other risks)?



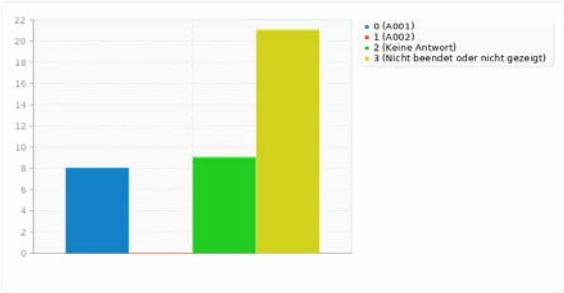
Zusammenfassung für Q001

Are you already performing due diligence and risk assessment for open source components you use in your products?

Antwort	Anzahl	Prozent
yes (A001)	8	21.05%
no (A002)	0	0.00%
Keine Antwort	9	23.68%
Nicht beendet oder nicht gezeigt	21	55.26%

Zusammenfassung für Q001

Are you already performing due diligence and risk assessment for open source components you use in your products?



Zusammenfassung für Q002

Do you have a backup plan (what plan?) if some of the critical open source projects you rely on will be abandoned by maintainers?

Antwort	Anzahl	Prozent
Antwort	7	18.42%
Keine Antwort	10	26.32%
Nicht beendet oder nicht gezeigt	21	55.26%

ID	Antwort
39	Other than looking for alternatives should it happen: No
44	y
49	No
52	In our case this is in the hands of our product architects and hardware platform providers. Generally stability and veracity of critical components is checked prior to adoption.
57	yes, for critical projects we have hired staff to take over
64	We continue minimal support on our own. Or we'll select alternative project
69	no

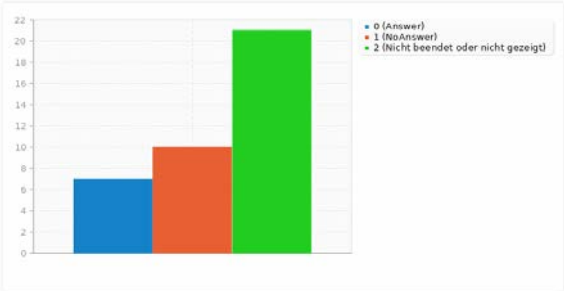
Zusammenfassung für Q003

Do you plan to fork/maintain open source projects because of the CRA?

Antwort	Anzahl	Prozent
yes (A001)	2	5.26%
no (A002)	7	18.42%
Keine Antwort	8	21.05%
Nicht beendet oder nicht gezeigt	21	55.26%

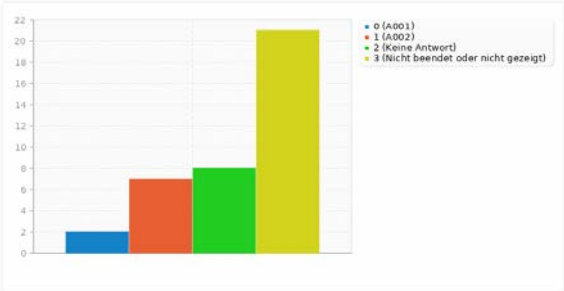
Zusammenfassung für Q002

Do you have a backup plan (what plan?) if some of the critical open source projects you rely on will be abandoned by maintainers?



Zusammenfassung für Q003

Do you plan to fork/maintain open source projects because of the CRA?



Zusammenfassung für Q004

Are you planning to replace open source projects with proprietary software because of the CRA?

Antwort	Anzahl	Prozent
yes (A001)	1	2.63%
no (A002)	7	18.42%
Keine Antwort	9	23.68%
Nicht beendet oder nicht gezeigt	21	55.26%

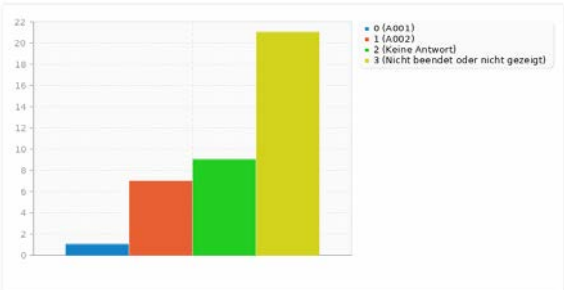
Zusammenfassung für Q020

Do you have a process for vulnerability management for your products that also covers open source dependencies so as to be compliant with CRA?

Antwort	Anzahl	Prozent
yes (A001)	8	21.05%
no (A002)	0	0.00%
Keine Antwort	9	23.68%
Nicht beendet oder nicht gezeigt	21	55.26%

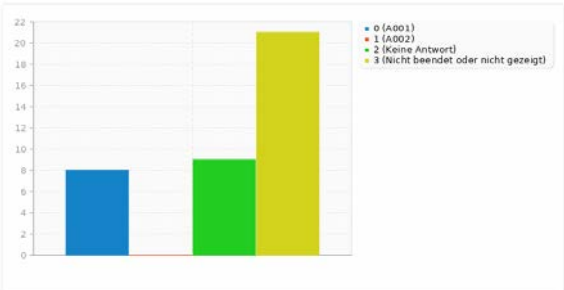
Zusammenfassung für Q004

Are you planning to replace open source projects with proprietary software because of the CRA?



Zusammenfassung für Q020

Do you have a process for vulnerability management for your products that also covers open source dependencies so as to be compliant with CRA?



Zusammenfassung für Q005

Are you already following regulations or standards in cybersecurity or SW security areas?

Antwort	Anzahl	Prozent
yes (A001)	5	13.16%
no (A002)	1	2.63%
Keine Antwort	8	21.05%
Nicht beendet oder nicht gezeigt	24	63.16%

Zusammenfassung für Q006

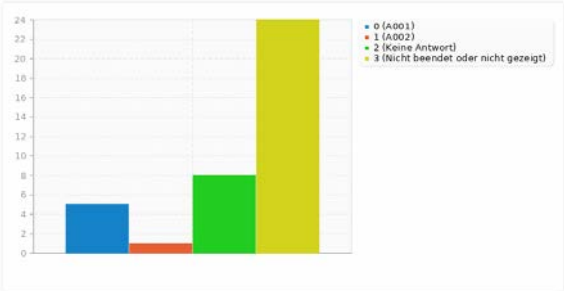
What regulations or standards are you following?

Antwort	Anzahl	Prozent
Antwort	4	10.53%
Keine Antwort	1	2.63%
Nicht beendet oder nicht gezeigt	33	86.84%

ID	Antwort
49	SSDF (formerly from US Executive Order)
57	Common Criteria, many security certifications, SLSA, openSSF's criticality assessment
64	iec18031, iec62443, iso27k
72	RED 3.3 Directive

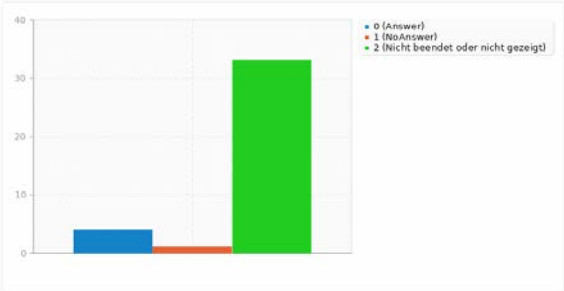
Zusammenfassung für Q005

Are you already following regulations or standards in cybersecurity or SW security areas?



Zusammenfassung für Q006

What regulations or standards are you following?



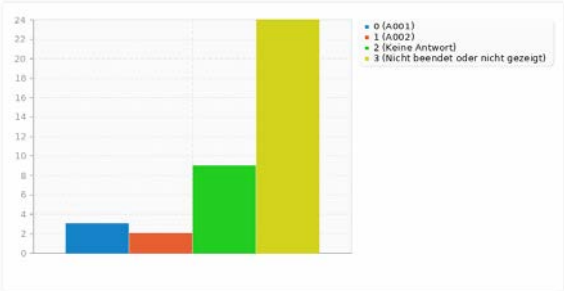
Zusammenfassung für Q007

Can it be ensured that the requirements of the CRA are met for the integrated open source components from the manufacturers own resources?

Antwort	Anzahl	Prozent
yes (A001)	3	7.89%
no (A002)	2	5.26%
Keine Antwort	9	23.68%
Nicht beendet oder nicht gezeigt	24	63.16%

Zusammenfassung für Q007

Can it be ensured that the requirements of the CRA are met for the integrated open source components from the manufacturers own resources?



Zusammenfassung für Q008

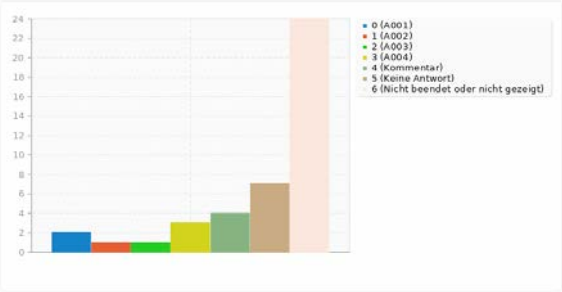
How do you deal with open source components that you do not know whether they fulfil the requirements of the CRA?

Antwort	Anzahl	Prozent
I ignore the project (A001)	2	5.26%
I contact the project/developer (A002)	1	2.63%
I help the project/invest in the project (A003)	1	2.63%
Other (A004)	3	7.89%
Kommentar	4	10.53%
Keine Antwort	7	18.42%
Nicht beendet oder nicht gezeigt	24	63.16%

ID	Antwort
39	I'm not aware of open source components having to fulfil any requirements. The requirements are on us, the manufacturer.
52	In our organization, the design-in of the open source software package is with the development teams, who reach out for approval to respective functions within the organization. Some of the questions in this questionaire would be for representatives in said other functions. During the selection of the packages for design-in the CRA is to be considered, to the extent we can/want to contribute and fix vulnerabilities we would partake in resolving and contribute.
64	we provide necessary support to customers on our own. It doesn't seem to be huge effort.
72	It is very difficult to contact all the project repository, There should be certificate map

Zusammenfassung für Q008

How do you deal with open source components that you do not know whether they fulfil the requirements of the CRA?



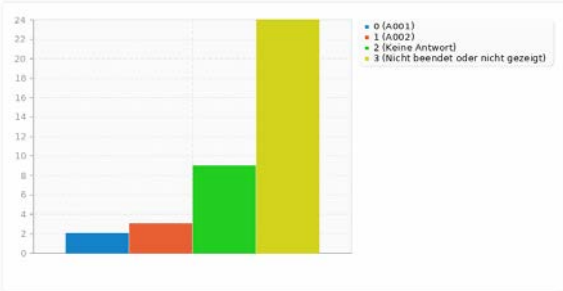
Zusammenfassung für Q009

Do you see requirements of the CRA for which it is difficult to ensure that the open source components integrated in the product fulfil them?

Antwort	Anzahl	Prozent
yes (A001)	2	5.26%
no (A002)	3	7.89%
Keine Antwort	9	23.68%
Nicht beendet oder nicht gezeigt	24	63.16%

Zusammenfassung für Q009

Do you see requirements of the CRA for which it is difficult to ensure that the open source components integrated in the product fulfil them?



Zusammenfassung für Q022

Which are these and why is it difficult?

Antwort	Anzahl	Prozent
Antwort	1	2.63%
Keine Antwort	1	2.63%
Nicht beendet oder nicht gezeigt	36	94.74%

ID	Antwort
72	Check EoL of the project

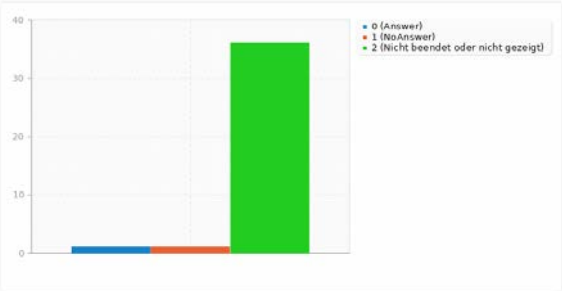
Zusammenfassung für Q010

Do you know who develops the open source components that you use in your products?

Antwort	Anzahl	Prozent
yes (A001)	4	10.53%
no (A002)	2	5.26%
Keine Antwort	8	21.05%
Nicht beendet oder nicht gezeigt	24	63.16%

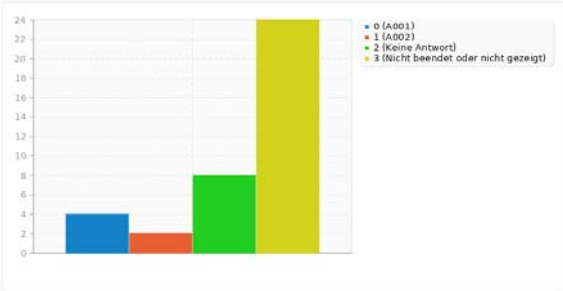
Zusammenfassung für Q022

Which are these and why is it difficult?



Zusammenfassung für Q010

Do you know who develops the open source components that you use in your products?



Zusammenfassung für Q011

Do you work with the providers of open source components that you know?

Antwort	Anzahl	Prozent
yes (A001)	2	5.26%
no (A002)	4	10.53%
Keine Antwort	8	21.05%
Nicht beendet oder nicht gezeigt	24	63.16%

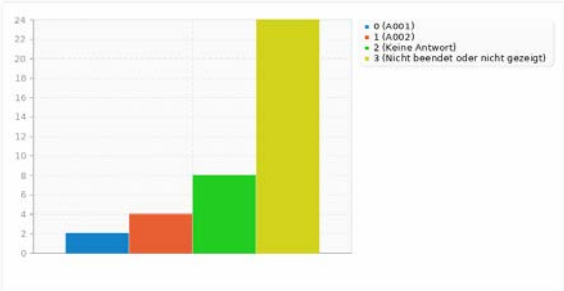
Zusammenfassung für Q012

Would proof that open source components fulfil the CRA requirements help?

Antwort	Anzahl	Prozent
yes (A001)	5	13.16%
no (A002)	1	2.63%
Keine Antwort	8	21.05%
Nicht beendet oder nicht gezeigt	24	63.16%

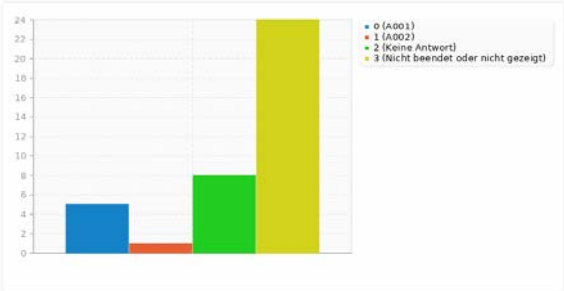
Zusammenfassung für Q011

Do you work with the providers of open source components that you know?



Zusammenfassung für Q012

Would proof that open source components fulfil the CRA requirements help?



Zusammenfassung für Q013

Is there a willingness to pay for them

Antwort	Anzahl	Prozent
yes (A001)	2	5.26%
no (A002)	0	0.00%
Keine Antwort	3	7.89%
Nicht beendet oder nicht gezeigt	33	86.84%

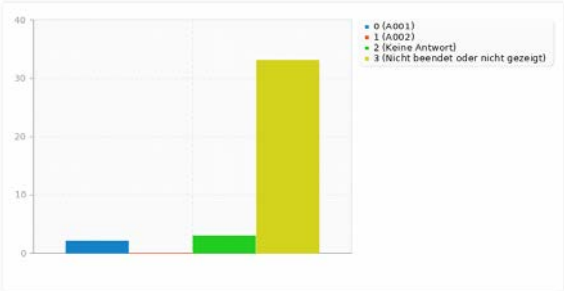
Zusammenfassung für Q014

Are you already working with potential stewards?

Antwort	Anzahl	Prozent
yes (A001)	3	7.89%
no (A002)	3	7.89%
Keine Antwort	8	21.05%
Nicht beendet oder nicht gezeigt	24	63.16%

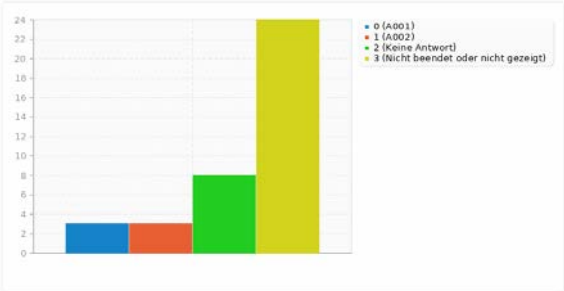
Zusammenfassung für Q013

Is there a willingness to pay for them



Zusammenfassung für Q014

Are you already working with potential stewards?



Zusammenfassung für Q015

Do you support them or are you planning to support them?

Antwort	Anzahl	Prozent
yes (A001)	2	5.26%
no (A002)	4	10.53%
Keine Antwort	8	21.05%
Nicht beendet oder nicht gezeigt	24	63.16%

Zusammenfassung für Q016

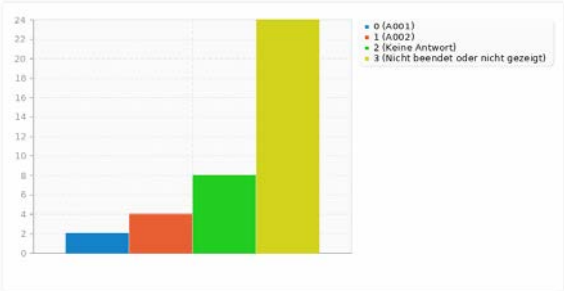
What does this support look like?

Antwort	Anzahl	Prozent
Antwort	1	2.63%
Keine Antwort	1	2.63%
Nicht beendet oder nicht gezeigt	36	94.74%

ID	Antwort
52	There are a number of projects that we actively contribute to (code submission/fixing/adding new features). This is a select number of projects, we do use code from (many) more projects than we contribute to (as is to be expected from a HW manufacturer using amongst others linux based HW platforms).

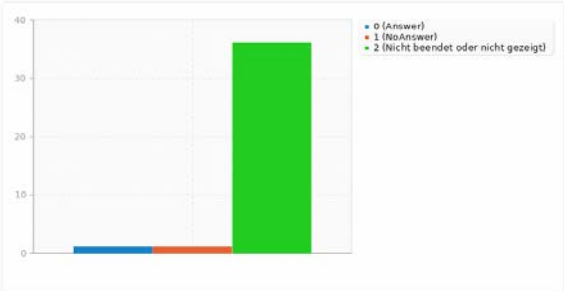
Zusammenfassung für Q015

Do you support them or are you planning to support them?



Zusammenfassung für Q016

What does this support look like?



Zusammenfassung für Q017

What support, and from whom, is needed to ensure that open source components in your products fulfill the CRA requirements?

Antwort	Anzahl	Prozent
Antwort	3	7.89%
Keine Antwort	7	18.42%
Nicht beendet oder nicht gezeigt	28	73.68%

ID	Antwort
52	- Support from the Semiconductor HW/SDK providers, in particular (as they determine the platform environment), - Support from SW/HW component suppliers in general, - Internally, development, security, legal, IP and OSS functions.
58	Coming from a bitkom post: I went through the survey twice but the questionnaire is not well made. Most are not really yes/no answers.
72	CRA compliance should be added in all open source project, to track them.

Zusammenfassung für Q018

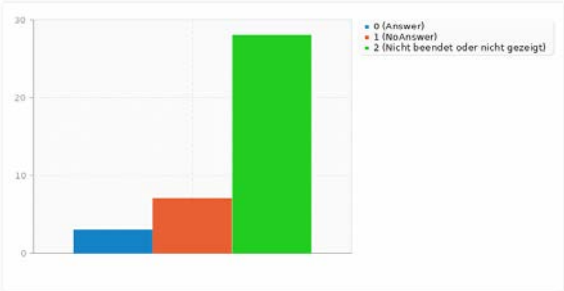
From the manufacturer's point of view, what can cooperation with open source look like (especially with the stewards)?

Antwort	Anzahl	Prozent
Antwort	1	2.63%
Keine Antwort	9	23.68%
Nicht beendet oder nicht gezeigt	28	73.68%

ID	Antwort
52	I suspect that the main cooperation would be a more proactive participation in fixing vulnerabilities. As this comes at a cost, it will likely affect the number of projects we can support and so this may result in more selective sourcing of code. It may in that regard result in a concentration of attention and usage by industry of select projects and/or platform. It may thus result in less diversity...

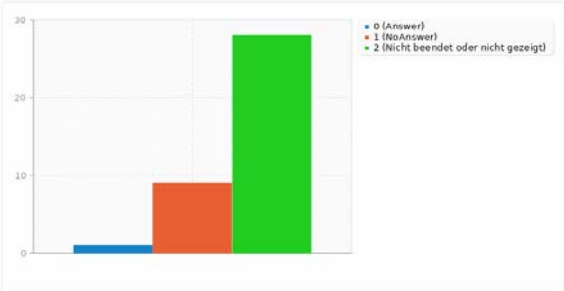
Zusammenfassung für Q017

What support, and from whom, is needed to ensure that open source components in your products fulfill the CRA requirements?



Zusammenfassung für Q018

From the manufacturer's point of view, what can cooperation with open source look like (especially with the stewards)?



Zusammenfassung für Q021

What agreements should be made?

Antwort	Anzahl	Prozent
Antwort	1	2.63%
Keine Antwort	9	23.68%
Nicht beendet oder nicht gezeigt	28	73.68%

ID	Antwort
52	Although things might differ for different stewards, but I do not expect that the CRA will result in many agreements with stewards. I suspect that most manufacturers will in their supply agreements push - obligations towards their suppliers that provide a platform - which suppliers in their turn will select well-maintained platforms and most likely contribute to those resulting in a "monoculture" of standardized industry supported packages under preferably permissive licenses. I do not foresee that the CRA will lead to the rise of OSS stewards as contractors for businesses - it might, but as many manufacturers will have similar interests, this might actually result in consolidation in select standard works comparable to say Linux and OpenSSL being adopted and supported by industry as a whole, leaving other non-adopted projects for what they are. But hey I might be completely wrong *:)

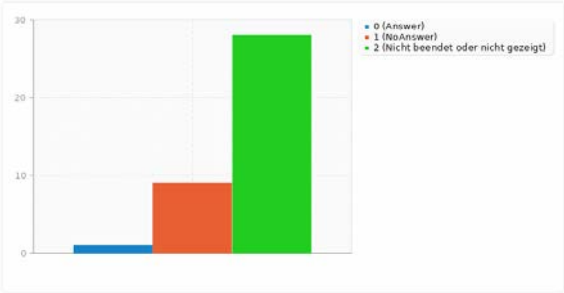
Zusammenfassung für Q019

From the manufacturer's point of view, is legal advice required for collaboration with stewards / open source projects?

Antwort	Anzahl	Prozent
yes (A001)	2	5.26%
no (A002)	2	5.26%
Keine Antwort	6	15.79%
Nicht beendet oder nicht gezeigt	28	73.68%

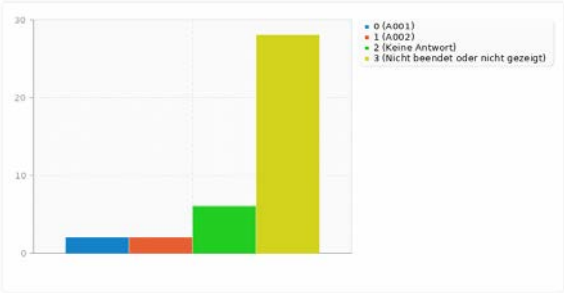
Zusammenfassung für Q021

What agreements should be made?



Zusammenfassung für Q019

From the manufacturer's point of view, is legal advice required for collaboration with stewards / open source projects?



Fragebogen für OSS-Projekte in Bezug auf den CRA

Ergebnisse

Umfrage 323741

Anzahl der Datensätze in dieser Abfrage:	65
Gesamtzahl der Datensätze dieser Umfrage:	65
Anteil in Prozent:	100.00%

Zusammenfassung für Q00

Wisst ihr, welche Rolle ihr unter dem CRA einnehmen werdet?

Antwort	Anzahl	Prozent
ja (A001)	7	10.77%
nein (A002)	14	21.54%
Keine Antwort	8	12.31%
Nicht beendet oder nicht gezeigt	36	55.38%

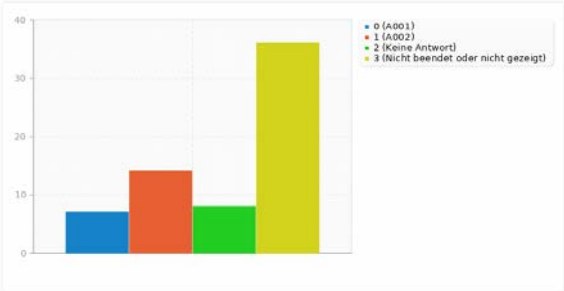
Zusammenfassung für Q001

Welche Rolle ist das?

Antwort	Anzahl	Prozent
Ich falle nicht unter den CRA (A004)	5	7.69%
Ich bin ein Open Source Steward (A005)	1	1.54%
Ich bin ein Hersteller (A006)	1	1.54%
Keine Antwort	0	0.00%
Nicht beendet oder nicht gezeigt	58	89.23%

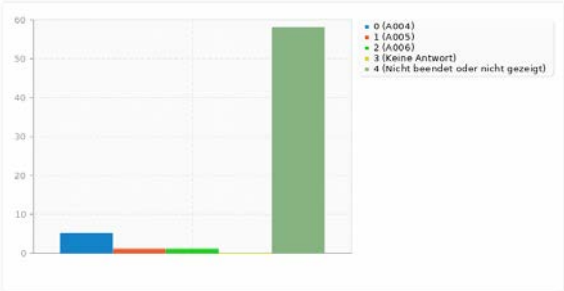
Zusammenfassung für Q00

Wisst ihr, welche Rolle ihr unter dem CRA einnehmen werdet?



Zusammenfassung für Q001

Welche Rolle ist das?



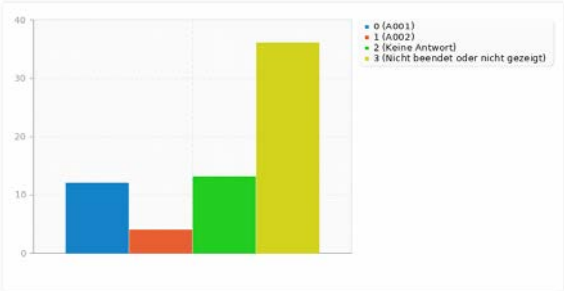
Zusammenfassung für Q002

Möchten Sie erklären/antworten können, dass Sie als Mitwirkender oder einzelner Betreuer nicht in den Geltungsbereich der CRA-Verpflichtungen fallen?

Antwort	Anzahl	Prozent
ja (A001)	12	18.46%
nein (A002)	4	6.15%
Keine Antwort	13	20.00%
Nicht beendet oder nicht gezeigt	36	55.38%

Zusammenfassung für Q002

Möchten Sie erklären/antworten können, dass Sie als Mitwirkender oder einzelner Betreuer nicht in den Geltungsbereich der CRA-Verpflichtungen fallen?



Zusammenfassung für Q003

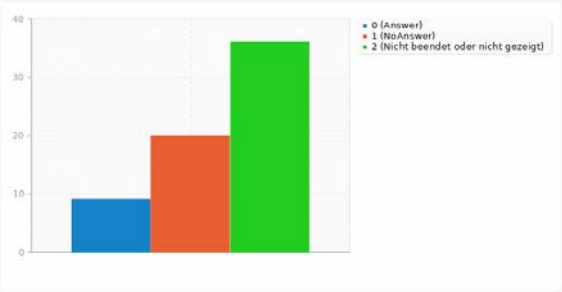
Welche Fragen bezüglich des kommerziellen Hintergrunds ergeben sich für euer Projekt?

Antwort	Anzahl	Prozent
Antwort	9	13.85%
Keine Antwort	20	30.77%
Nicht beendet oder nicht gezeigt	36	55.38%

ID	Antwort
11	Open Source-Software (zwei Biblioheken für statische Programmanalyse), die primär für Forschung entwickelt wurden, aber auch in kommerziellen Produkten genutzt werden. Ich sehe hier keinen eindeutigen Steward. Muss dann jeder, der die OSS kommerziell nutzt, sie wie ein Teil seines Produkts behandeln? Was ist, wenn es dadurch zu Zielkonflikten kommt?
20	Wie kann ich als Open Source Beitragender ohne große Organisation dahinter mitwirken, dass Verstöße gegen den CRA reportet werden, wenn mir etwas auffällt?
36	Wir kriegen über alle kommerziellen Aktivitäten (App-Verkäufe, Online-Werbung, Spenden) nicht einmal 1/4 der Kosten auch nur eines potenziell festangestellten Programmierers herein, können aber immerhin Infrastrukturkosten etc. decken. Also effektiv rein kommerziell betrachtet ein reines Verlustgeschäft, wäre da nicht die ganze freiwillige, unbezahlte Arbeit. Haben wir die gleichen Verpflichtungen wie voll kommerzielle Hersteller? Falls nein, was ist für uns anders?
40	Gibt es evt. eine Geringfügigkeitsgrenze bzgl. der Monetarisierung des Projektes, deren Unterschreiten es uns ermöglichen würde, rechtlich nicht als Hersteller, sondern als Maintainer/Entwickler angesehen werden und wie hoch ist diese in EUR/Jahr?
45	Für meine Open Source Projekte gibt es von meiner Seite aus keinen kommerziellen Hintergrund. Ich entwickele diese Software weil es mir Spass macht. Sie ist Open Source, damit andere Leute sie verwenden können, ggf. auch in einem kommerziellen Umfeld.
47	Ab welchen Schritten der Kommerzialisierung muss ich Maßnahmen nach dem CRA ergreifen?
57	hä?
60	Wenn es nur einen einzigen "Sponsor" gibt, ist es dann kommerziell?
61	Wir sind sehr unsicher, ab wo genau sich ein "kommerzieller Hintergrund" ergeben würde. Es gibt kommerzielle Anbieter rund um das Produkt, Schulung, Hosting, Weiterentwicklung. Die sind auch als Mitglieder (neben anderen) in einem gemeinnützigen e.V. organisiert. Auch die Gemeinnützigkeit des Vereins steht bisweilen in Frage, wir vermuten, dass bezüglich CRA die gleichen Probleme/Fragen auf uns zukommen könnten.

Zusammenfassung für Q003

Welche Fragen bezüglich des kommerziellen Hintergrunds ergeben sich für euer Projekt?



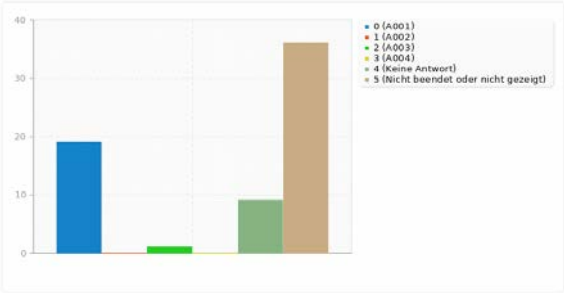
Zusammenfassung für Q004

Wenn Sie Spenden für ein Open-Source-Projekt, das Sie betreuen, entgegennehmen, schätzen Sie, dass diese niedriger, fast gleich hoch, höher oder deutlich höher sind als die tatsächlichen Kosten für Entwicklung und Wartung?

Antwort	Anzahl	Prozent
niedriger (A001)	19	29.23%
fast gleich hoch (A002)	0	0.00%
höher (A003)	1	1.54%
deutlich höher (A004)	0	0.00%
Keine Antwort	9	13.85%
Nicht beendet oder nicht gezeigt	36	55.38%

Zusammenfassung für Q004

Wenn Sie Spenden für ein Open-Source-Projekt, das Sie betreuen, entgegennehmen, schätzen Sie, dass diese niedriger, fast gleich hoch, höher oder deutlich höher sind als die tatsächlichen Kosten für Entwicklung und Wartung?



Zusammenfassung für Q005

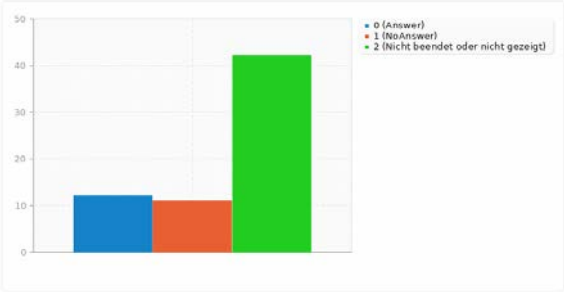
Gibt es etwas, dass euch das Gefühl vermittelt, dass ihr die Anforderungen des CRA erfüllen müsst?

Antwort	Anzahl	Prozent
Antwort	12	18.46%
Keine Antwort	11	16.92%
Nicht beendet oder nicht gezeigt	42	64.62%

ID	Antwort
11	Indirekt dadurch, dass die OSS in kommerziellen Produkten genutzt wird. Hierdurch kann seitens der kommerziellen Nutzer Druck auf das OSS-Projekt entstehen
20	Nein
21	nein
24	Compliance-Anforderungen von Business-Nutzern
36	wir nutzen App-Verkäufe & Online-Werbung für kommerzielle Einnahmen; wir erhalten geringe Mengen an Spenden (meist < 100€/Monat)
40	nein
42	Unsicherheit, ob ich von CRA betroffen bin.
43	Unklarheit in der rechtlichen Praxis
45	Nein, ich war mehrfach auf der FOSDEM Konferenz und habe Vorträge zum CRA gehört. Nach meinem besten Wissen bin ich von keiner Anforderung des CRA betroffen.
47	Die unklare Definition für "Produkte".
50	Jain, die Anforderungen sind relativ klar und recht offensichtlich, aber andererseits einfach für den normalen geregelten Betrieb notwendig. Wenn jemand offensichtlich in den Bereich fällt wo die Anforderungen relevant werden, gehen sie nicht über "normale" Anforderungen hinaus, die sowieso jeder Entwickler im entsprechenden Bereich beachten muss.
61	Ja. Auf der einen Seite die Unsicherheit bezüglich der kommerziellen Tätigkeit. Wir nehmen an, dass wir im Zweifel nicht wissen, ob wir Steward oder Manufacturer sind, bis wir von einer Marktaufsicht auf eines der beiden gecalled werden. Außerdem nehmen wir an, dass es Anspruchsinhaber geben könnte, aus der Community oder bei den Kunden, die verlangen, dass wir die Manufacturer-Anforderungen erfüllen, egal ob wir müssten oder nicht.

Zusammenfassung für Q005

Gibt es etwas, dass euch das Gefühl vermittelt, dass ihr die Anforderungen des CRA erfüllen müsst?



Zusammenfassung für Q006

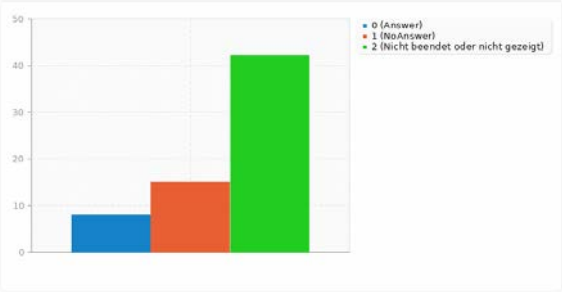
Welche Vorgaben (Guidance/Standards) würdet ihr für eine freiwillige Erfüllung der CRA Anforderungen benötigen?

Antwort	Anzahl	Prozent
Antwort	8	12.31%
Keine Antwort	15	23.08%
Nicht beendet oder nicht gezeigt	42	64.62%

ID	Antwort
11	Schwierig, weil die OSS sehr generisch ist und teilweise auf anderer (legacy) OSS aufbaut
20	Infos, wie wir bei Verstößen reagieren müssen und wer uns hier helfen kann.
40	Wie genau muss ich meine Benutzer über Sicherheitsprobleme im Produkt informieren? Website/Mailingliste/andere? Ein wesentliches Kennzeichen von OSS ist, dass die Maintainer ihre Benutzer oft überhaupt nicht kennen - denn die Software kann frei und kostenlos verwendet werden. Nur ein verschwindend geringer Anteil der Verwender tritt jemals mit den Maintainern in Kontakt. Eine vom Maintainer initiierte Kontaktaufnahme ist daher schwierig.
43	Möglichst breite FAQs und rechtliche Beratung
45	Keine - würde der CRA zu bedeutender Mehrarbeit führen, würde ich die Projekte von GitHub löschen!
47	Eine Checkliste der Anforderungen mit Erläuterungen
50	Keine, die "GRUNDLEGENDE CYBERSECURITYANFORDERUNGEN" sind in ihrer Allgemeinheit und Kürze klar verständlich und benötigen keine weitere Ausführung oder Interpretation.
61	Für unsere wäre eine konkretisierte Richtlinie zur Umsetzung sicherlich hilfreich, oder vielleicht auch Best-Practice-Beispiele. Wir vermuten allerdings, das wir aufgrund der organisatorischen Struktur unserer Community, ohnehin einen Teil der Anforderungen für uns selbst geeignet interpretieren und implementieren müssen.

Zusammenfassung für Q006

Welche Vorgaben (Guidance/Standards) würdet ihr für eine freiwillige Erfüllung der CRA Anforderungen benötigen?



Zusammenfassung für Q007

Glauben Sie, dass Sie bereits fast alles tun, was zur Erfüllung der CRA-Anforderungen erforderlich ist (auch wenn dies freiwillig geschieht)?

Antwort	Anzahl	Prozent
ja (A001)	4	6.15%
nein (A002)	11	16.92%
Keine Antwort	8	12.31%
Nicht beendet oder nicht gezeigt	42	64.62%

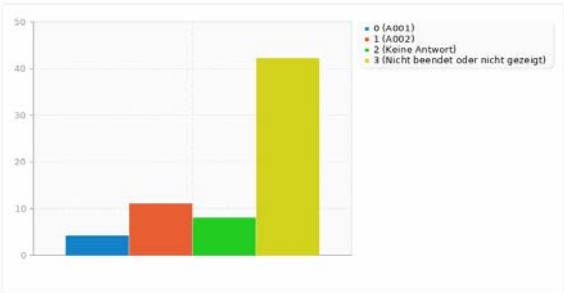
Zusammenfassung für Q008

Könnt ihr euch vorstellen, dass jemand für euer Projekt die Rolle des Stewards übernimmt?

Antwort	Anzahl	Prozent
ja (A001)	2	3.08%
nein (A002)	11	16.92%
Keine Antwort	6	9.23%
Nicht beendet oder nicht gezeigt	46	70.77%

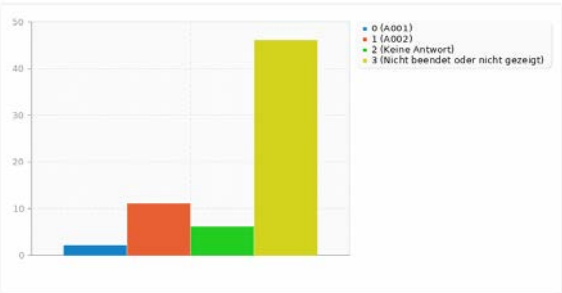
Zusammenfassung für Q007

Glauben Sie, dass Sie bereits fast alles tun, was zur Erfüllung der CRA-Anforderungen erforderlich ist (auch wenn dies freiwillig geschieht)?



Zusammenfassung für Q008

Könnt ihr euch vorstellen, dass jemand für euer Projekt die Rolle des Stewards übernimmt?



Zusammenfassung für Q009

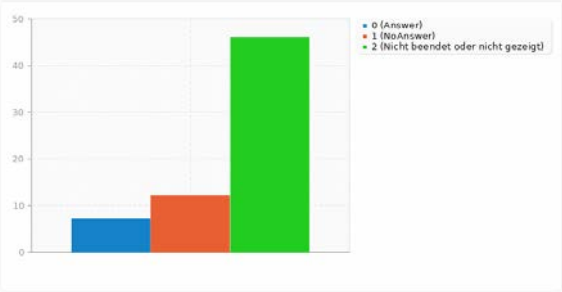
Wen könnt ihr euch als Steward für euer Projekt vorstellen?

Antwort	Anzahl	Prozent
Antwort	7	10.77%
Keine Antwort	12	18.46%
Nicht beendet oder nicht gezeigt	46	70.77%

ID	Antwort
11	eigentlich nur Unis oder Forschungseinrichtungen, die dafür aber öffentliche Fördermittel bräuchten
20	Ja. Aber leider haben wir keine große Foundation hinter uns und einzelne Personen sind nicht erlaubt.
40	Wir würden keinen externen Steward akzeptieren um Kontrollverlust zu vermeiden; außerdem ist fraglich, warum jemand externes diese Dienstleistung übernehmen sollte, ohne dass monetäre Motivation dahintersteckt - was wiederum für uns zum Problem würde, weil das Entwickeln des Produkts eben gerade NICHT hauptsächlich monetär motiviert war. Da besteht ein Zielkonflikt.
42	Jemand, der genügend Umsatz erzielt und die regulatorischen Belastungen tragen zu können
43	Eine Person in den USA
45	N/A
61	Ja, allerdings nur insofern als das wir die organisatorische Struktur (Verein, Community) unseres Projektes geeignet weiterentwicklen, so dass wir sicher Steward sind. Wir können uns nicht vorstellen, uns irgendwo anzuschließen.

Zusammenfassung für Q009

Wen könnt ihr euch als Steward für euer Projekt vorstellen?



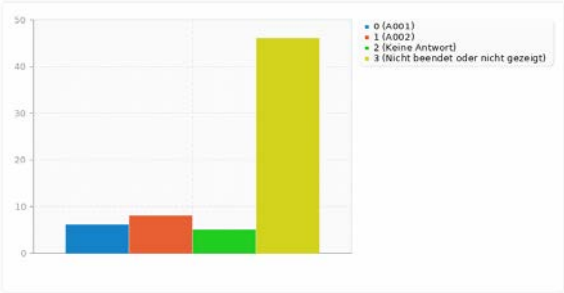
Zusammenfassung für Q010

Könnt ihr euch vorstellen, die Rolle des Stewards selbst zu übernehmen?

Antwort	Anzahl	Prozent
ja (A001)	6	9.23%
nein (A002)	8	12.31%
Keine Antwort	5	7.69%
Nicht beendet oder nicht gezeigt	46	70.77%

Zusammenfassung für Q010

Könnt ihr euch vorstellen, die Rolle des Stewards selbst zu übernehmen?



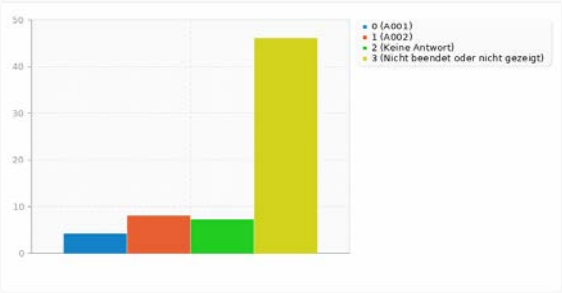
Zusammenfassung für Q011

Haben Sie das Gefühl, dass Sie wegen dem CRA einem Steward beitreten (oder ein Steward werden) müssen?

Antwort	Anzahl	Prozent
ja (A001)	4	6.15%
nein (A002)	8	12.31%
Keine Antwort	7	10.77%
Nicht beendet oder nicht gezeigt	46	70.77%

Zusammenfassung für Q011

Haben Sie das Gefühl, dass Sie wegen dem CRA einem Steward beitreten (oder ein Steward werden) müssen?



Zusammenfassung für Q012

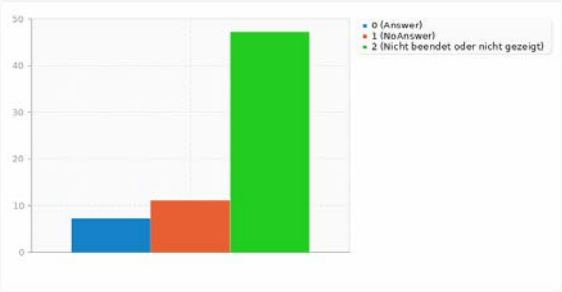
Welche Hilfe benötigen Sie als Betreuer am dringendsten (von Steward, Hersteller, Regulierungsbehörden, Sponsorunternehmen, Leitern von Schwachstellenprogrammen usw.), um Ihr Projekt für Ihre Benutzer attraktiver zu machen, da diese die Einhaltung der CRA-Vorschriften möglicherweise als Voraussetzung für die Annahme betrachten?

Antwort	Anzahl	Prozent
Antwort	7	10.77%
Keine Antwort	11	16.92%
Nicht beendet oder nicht gezeigt	47	72.31%

ID	Antwort
11	Fördermittel. Bei OSS aus akademischen Einrichtungen läuft irgendwann das Förderprojekt aus, auf dem die OSS entwickelt wurde. Es ist im Fördersystem nicht vorgesehen, Software etwas nachhaltig zu pflegen. Es gibt zwar neuerdings Calls für Software-Infrastruktur, aber da wird einerseits von Nachhaltigkeit im Sinne von "soll weiterleben" gesprochen, andererseits sind das aber auch nur Mittel für sehr kurze begrenzte Zeit.
24	Zeit
36	einfache Auflistung der Verpflichtungen; praxisrelevante Beispiele von kleinen OSS-Projekten & typischen Fällen wie Online-Werbung, App-Verkäufe, Spendeneinnahmen
40	Idealerweise gäbe es eine vom Bund bereitgestellte Infrastruktur, die deutsche OSS-Projekte kostenlos nutzen können, um wesentliche Anforderungen des CRA zu erfüllen. Eine Analogie sehe ich bspw. in GitHub's Behauptung, durch Verwendung Ihrer Infrastrktur SLSA Level 3 Compliance erreichen zu können. Wenn der Bund/die EU bspw. eine zentrale Plattform fürs Meldewesen von Schwachstellen für Hersteller in Richtung ihrer Benutzer anbieten würde, wäre das super.
43	Rechtliche Klarheit
45	Klare Informationen, wann bzw. in wie fern man vom CRA betroffen ist. Niemand will 80 Seiten im Original lesen, Wenn es keine einfach Zusammenfassung und klare Handlungstipps gibt, werden viele OSS Projekt auch nichts machen.
61	Vermutlich werden wir einfach entsprechende Ressourcen, als finanzielle Mittel oder in Form von Expertise, benötigen. Wir sind ständig unterfinanziert, werden aber in vielen deutschen öffentlichen Einrichtungen genutzt.

Zusammenfassung für Q012

Welche Hilfe benötigen Sie als Betreuer am dringendsten (von Steward, Hersteller, Regulierungsbehörden, Sponsorunternehmen, Leitern von Schwachstellenprogrammen usw.), um Ihr Projekt für Ihre Benutzer attraktiver zu machen, da diese die Einhaltung der CRA-Vorschriften möglicherweise als Voraussetzung für die Annahme betrachten?



Zusammenfassung für Q013

Gibt es jetzt schon Unterstützungsleistungen, die ihr bekommt?

Antwort	Anzahl	Prozent
ja (A001)	3	4.62%
nein (A002)	12	18.46%
Keine Antwort	3	4.62%
Nicht beendet oder nicht gezeigt	47	72.31%

Zusammenfassung für Q016

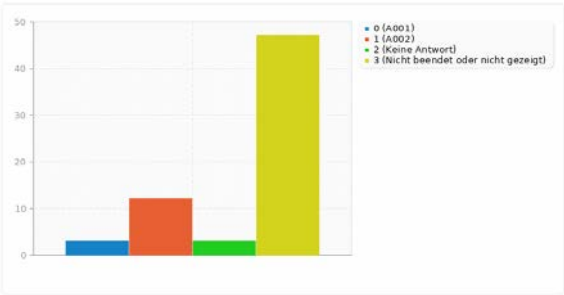
Welche sind das?

Antwort	Anzahl	Prozent
Antwort	3	4.62%
Keine Antwort	0	0.00%
Nicht beendet oder nicht gezeigt	62	95.38%

ID	Antwort
11	kurze Förderprogramme z.B. über die DFG, um ganz spezifische Vorhaben umzusetzen, z.B. eine konkrete Weiterentwicklung. In diesem Kontext kann man dann z.B. auch Anforderungen aus Annex 1 umsetzen, aber auch nur, solange es ins Budget passt (das Geld ist ja eigentlich für die Weiterentwicklung) und solange das zeitlich begrenzte Geld überhaupt fließt.
20	Sponsoring über die (kleine) Geeko Foundation und von SUSE
61	Gelegentlich werden wir über Landes- oder Bundesprojekte finanziert.

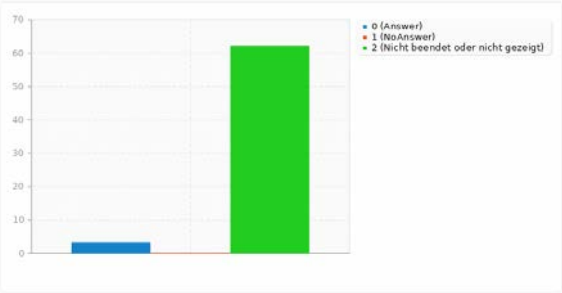
Zusammenfassung für Q013

Gibt es jetzt schon Unterstützungsleistungen, die ihr bekommt?



Zusammenfassung für Q016

Welche sind das?



Zusammenfassung für Q014

Von wem bekommt ihr diese Unterstützungsleistung?

Antwort	Anzahl	Prozent
Antwort	4	6.15%
Keine Antwort	14	21.54%
Nicht beendet oder nicht gezeigt	47	72.31%

ID	Antwort
11	öffentliche Fördermittelgeber
20	Geeko Foundation
45	N/A
61	Unterschiedliche Projektträger aus dem öffentlichen Bereich.

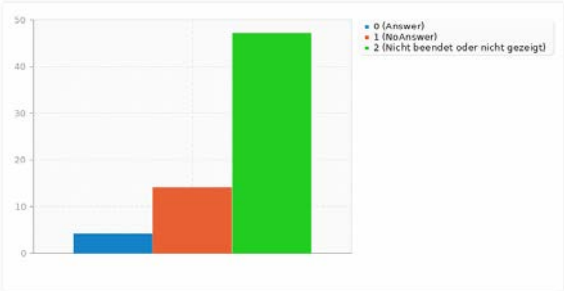
Zusammenfassung für Q015

Könnte diese Unterstützung jetzt schon bei der Erfüllung der CRA Anforderungen helfen?

Antwort	Anzahl	Prozent
yes (A001)	1	1.54%
no (A002)	5	7.69%
Keine Antwort	12	18.46%
Nicht beendet oder nicht gezeigt	47	72.31%

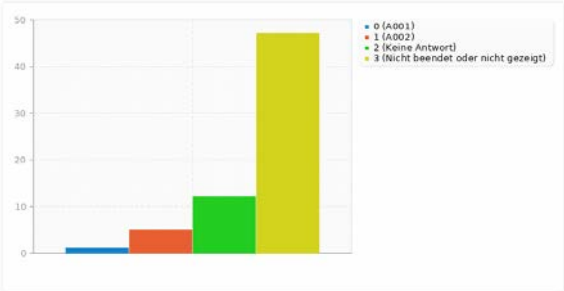
Zusammenfassung für Q014

Von wem bekommt ihr diese Unterstützungsleistung?



Zusammenfassung für Q015

Könnte diese Unterstützung jetzt schon bei der Erfüllung der CRA Anforderungen helfen?



Questionnaire for OSS Projects Maintainers in terms of CRA

Ergebnisse

Umfrage 241948

Anzahl der Datensätze in dieser Abfrage:	96
Gesamtzahl der Datensätze dieser Umfrage:	96
Anteil in Prozent:	100.00%

Zusammenfassung für Q001

Do you know what your role will be under the CRA?

Antwort	Anzahl	Prozent
yes (A001)	15	15.62%
no (A002)	15	15.62%
Keine Antwort	24	25.00%
Nicht beendet oder nicht gezeigt	42	43.75%

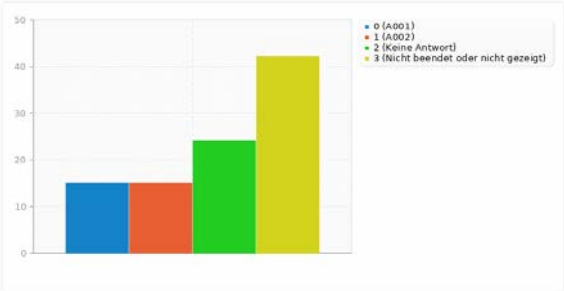
Zusammenfassung für Q002

What is your role?

Antwort	Anzahl	Prozent
I do not fall under the CRA (A001)	8	8.33%
I am a steward (A002)	3	3.12%
I am a manufacturer (A003)	3	3.12%
Keine Antwort	1	1.04%
Nicht beendet oder nicht gezeigt	81	84.38%

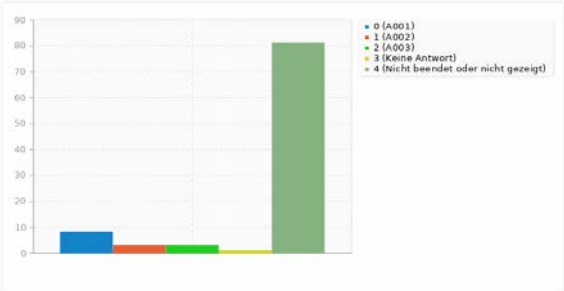
Zusammenfassung für Q001

Do you know what your role will be under the CRA?



Zusammenfassung für Q002

What is your role?



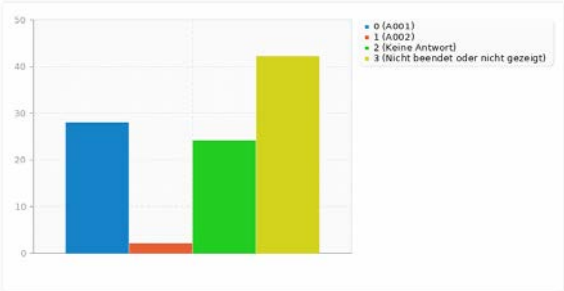
Zusammenfassung für Q003

Do you want to be able to declare/respond that you as a contributor or individual maintainer are out of scope for CRA obligations?

Antwort	Anzahl	Prozent
yes (A001)	28	29.17%
no (A002)	2	2.08%
Keine Antwort	24	25.00%
Nicht beendet oder nicht gezeigt	42	43.75%

Zusammenfassung für Q003

Do you want to be able to declare/respond that you as a contributor or individual maintainer are out of scope for CRA obligations?



Zusammenfassung für Q004

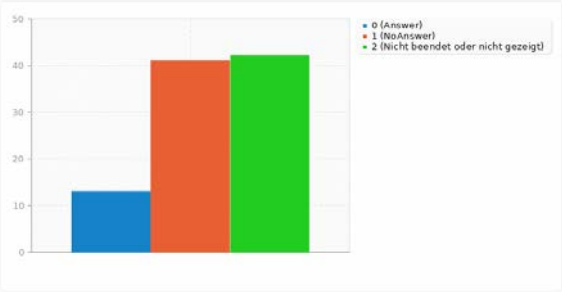
What questions regarding the commercial background arise for your project?

Antwort	Anzahl	Prozent
Antwort	13	13.54%
Keine Antwort	41	42.71%
Nicht beendet oder nicht gezeigt	42	43.75%

ID	Antwort
17	at what point would I be considered a manufacturer. what does "intend to make a profit" mean exactly and how is "profit" determined and defined
35	Background: the "project" is just a loosely organized bunch of individuals, there's no legal entity. But: members of the project work for companies that provide commercial support and development around "project". What does that mean for "project" wrt to CRA?
47	How does it work when you do not want to run your open source project with a commercial background? Having legal deadlines without getting paid is not very nice. Maintenance is normally not paid, if you do not do fundraising campaigns something between 0% and 5%.
50	I don't understand responsibilities and legal liability relative to where commercialisation is taking place. For example, if commercial activities are under a separate legal entity, but the project itself remains under my personal control & maintainership, am I personally liable due to commercialisation of a technically separate legal entity?
54	I am making money from Open Source development. This probably makes me a manufacturer. I can not fulfill the roles of a manufacturer unless I get paid a lot more money, but it is unlikely that anybody will do that. So it is unclear how I can keep my marginal business afloat.
59	Am I/are we as a FOSS community facing incalculable risks? Would that help proprietary vendors get rid of FOSS competition?
60	None of my projects have a "commercial background", but for sure any downstream users or forks may.
62	Our work requires purchasing of industry equipment. For that we ask for donations. I'm a bit unsure, if it's then considered "commercial activity"
75	I want to run my project (OpenPrinting) as a non-for-profit organization and receive donations/sponsorships/membership fees. Am I still considered non-commercial then and so I am still exempt from the CRA?
82	No commercial background
85	How much money and how can anyone earn/charge for project related activities before the project is suddenly considered a "manufacturer"?
86	How can we sure that those forking our projects and commercialising them are contributing back to the manufacturer, particularly when it comes to the added CRA responsibilities?
88	I avoid anything that might be commercial. No donations, no support agreements.

Zusammenfassung für Q004

What questions regarding the commercial background arise for your project?



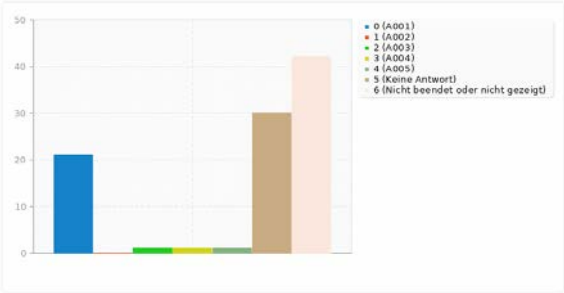
Zusammenfassung für Q007

If you're taking donations for an open source project that you maintain, do you assess they are lower, almost the same, bigger or significantly bigger than the actual costs of development and maintenance?

Antwort	Anzahl	Prozent
lower (A001)	21	21.88%
almost the same (A002)	0	0.00%
bigger (A003)	1	1.04%
significantly bigger (A004)	1	1.04%
(A005)	1	1.04%
Keine Antwort	30	31.25%
Nicht beendet oder nicht gezeigt	42	43.75%

Zusammenfassung für Q007

If you're taking donations for an open source project that you maintain, do you assess they are lower, almost the same, bigger or significantly bigger than the actual costs of development and maintenance?



Zusammenfassung für Q008

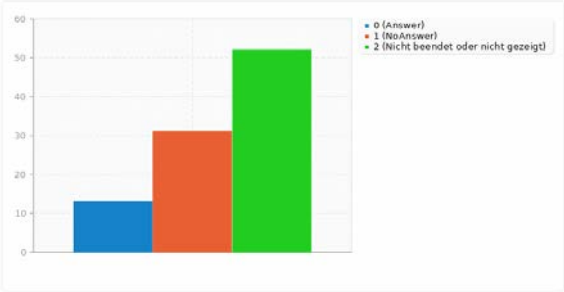
Is there anything that makes you feel that you have to fulfil the requirements of the CRA?

Antwort	Anzahl	Prozent
Antwort	13	13.54%
Keine Antwort	31	32.29%
Nicht beendet oder nicht gezeigt	52	54.17%

ID	Antwort
3	It's the law of my country.
7	For some vulnerabilities, technical project team members/devs are the only ones capable of promptly diagnosing and fixing the issues. e.g. log4j. or https://lwn.net/SubscriberLink/1025971/73f269ad3695186d/ So yes, as a conscientious member of the project/technical team I feel an obligation to the manufacturers and other consumers (e.g. other open source projects) to maintain the quality of the software (including security). If the CRA is has the power of law, however, then i expect that without some explicit disavowal, I would be forced by the law to perform maintenance and meet other legal requirements.
35	What makes you a steward and what are the obligations?
38	No
47	No
54	I am making money selling Open Source software that I write.
59	Rumours.
60	No.
62	Well... I'm a German citizen, writing software for the European market.
75	If I am running OpenPrinting as a non-for-profit organization and get funded, do I still not need to fulfill the requirements of the CRA (as I am still an open-source organization)?
78	Fear of breaking the law because of complexity and unclear requirements
82	No
88	In general the existence of a regulation that places duties on volunteers is uncomfortable. I'd like to see it super clear that non-commercial projects have zero requirements.

Zusammenfassung für Q008

Is there anything that makes you feel that you have to fulfil the requirements of the CRA?



Zusammenfassung für Q009

What guidance/standards would you need for voluntary compliance with the CRA requirements?

Antwort	Anzahl	Prozent
Antwort	8	8.33%
Keine Antwort	36	37.50%
Nicht beendet oder nicht gezeigt	52	54.17%

ID	Antwort
3	Better clarification of the requirements for stewards.
7	No guidance or standards necessary. Most will be perceived as an 'unpaid mandate'.
	What's actually required: $$$/support for the maintenance/technical work, and rational/not fantasy-based CRA requirements.
35	Explain how CRA applies to software projects, including any obligations.
54	There is nothing "voluntary" about the CRA. I don't understand the question.
59	Clear checklists and funding for additional efforts.
60	Tooling for generating SBOMs automatically, preferably very easy to integrate in CI pipelines.
75	I need to know whether the common practice of current open source and OS distributions (CVEs, non-disclosure to give the distros time to include/make available the fix, ...) is good enough for the CRA or whether more is needed and what is needed.
82	I see no reason to.

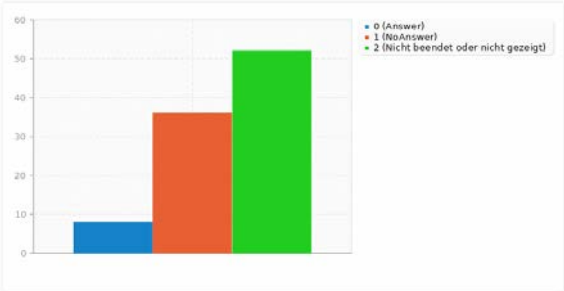
Zusammenfassung für Q010

Do you think you do almost everything already that's needed to fulfill CRA requirements (even if voluntary)?

Antwort	Anzahl	Prozent
yes (A001)	13	13.54%
no (A002)	5	5.21%
Keine Antwort	26	27.08%
Nicht beendet oder nicht gezeigt	52	54.17%

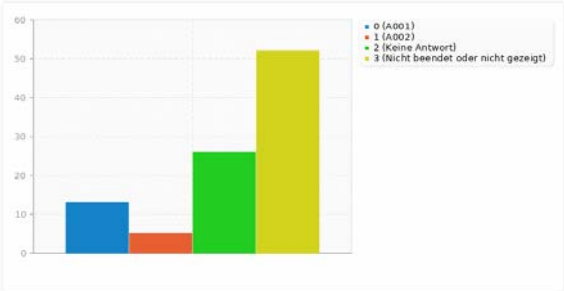
Zusammenfassung für Q009

What guidance/standards would you need for voluntary compliance with the CRA requirements?



Zusammenfassung für Q010

Do you think you do almost everything already that's needed to fulfill CRA requirements (even if voluntary)?



Zusammenfassung für Q013

Can you imagine someone taking on the steward role for your project?

Antwort	Anzahl	Prozent
yes (A001)	7	7.29%
no (A002)	14	14.58%
Keine Antwort	18	18.75%
Nicht beendet oder nicht gezeigt	57	59.38%

Zusammenfassung für Q014

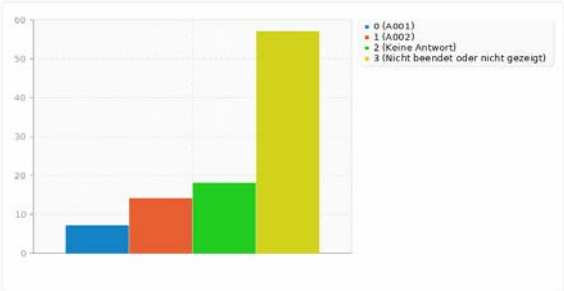
Who can you imagine as a steward for your project?

Antwort	Anzahl	Prozent
Antwort	4	4.17%
Keine Antwort	3	3.12%
Nicht beendet oder nicht gezeigt	89	92.71%

ID	Antwort
3	Myself
35	Myself
54	Well, some organization that is willing to do that. I don't know of any fitting ones though that are already doing a job like that.
62	Myself

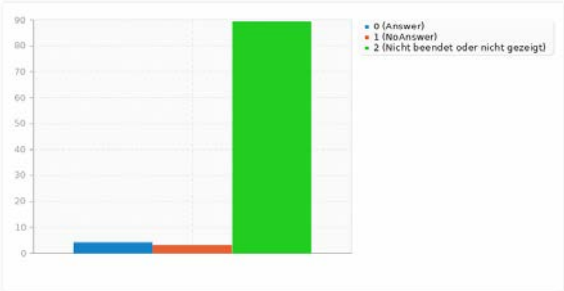
Zusammenfassung für Q013

Can you imagine someone taking on the steward role for your project?



Zusammenfassung für Q014

Who can you imagine as a steward for your project?



Zusammenfassung für Q015

Can you imagine taking on the steward role yourself?

Antwort	Anzahl	Prozent
yes (A001)	10	10.42%
no (A002)	11	11.46%
Keine Antwort	18	18.75%
Nicht beendet oder nicht gezeigt	57	59.38%

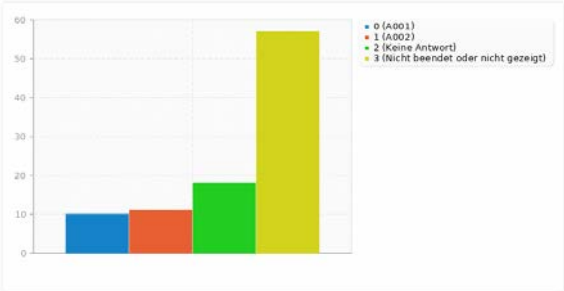
Zusammenfassung für Q017

Do you feel you must join one of the stewards (or become a steward) because of CRA?

Antwort	Anzahl	Prozent
yes (A001)	6	6.25%
no (A002)	10	10.42%
Keine Antwort	23	23.96%
Nicht beendet oder nicht gezeigt	57	59.38%

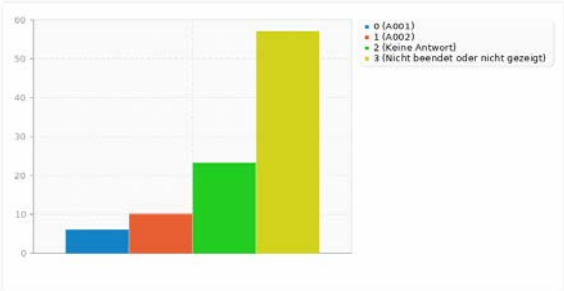
Zusammenfassung für Q015

Can you imagine taking on the steward role yourself?



Zusammenfassung für Q017

Do you feel you must join one of the stewards (or become a steward) because of CRA?



Zusammenfassung für Q018

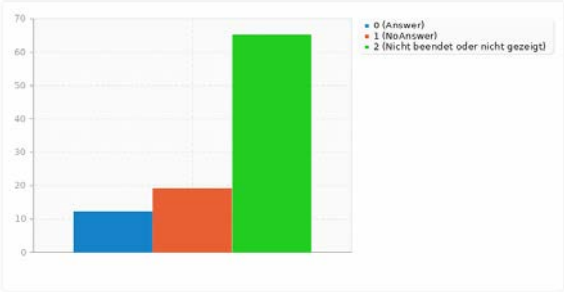
What help do you need most (from steward, manufacturer, regulators/authorities, sponsor companies, vulnerability program leaders, etc.) as a maintainer to make your project more attractive for your users, as they eventually may see CRA compliance as an adoption requirement?

Antwort	Anzahl	Prozent
Antwort	12	12.50%
Keine Antwort	19	19.79%
Nicht beendet oder nicht gezeigt	65	67.71%

ID	Antwort
35	Explain how CRA affects the software projects in simple terms and describe obligations.
47	If someone needs help with compliance they should pay someone for that. I am working on open source because I like software engineering, not to do management.
54	SBOM support for C++ is basically non-existent. So somebody needs to build the tools for that. From regulators I need clarity. And somebody has to pay for all of this.No.
59	Sustainable funds.
60	Whatever is needed to enable _them_ (each in their specific role) to utilise my project(s) in a CRA-compliant manner. If entities in each of the roles you mention (stewards, manufacturers, regulators / authorities, downstream users, vulnerability program leaders, etc.) do that, I assume my projects will automatically become CRA-compliant within a reasonable timespan.
62	Maintenance is more than just bugfixing. It requires cleaning up, refactoring etc. That's a lot of work. Compensation for that work would be great
75	Clear documentation about what are all the measures needed to fulfill CRA compliance, keeping updated about changes and new common practice and also keeping updated about incidents (like vulnerabilities) to which one needs to respond. Also funding for work which is required to acquire and maintain compliance.
78	Clear guidelines and a free hotline
85	sponsorship/support customers to help me pay developers
86	Financial support from corporations using the products we manufacture and guidance from regulators.
88	I actually don't care who adopts or doesn't.
89	Funding

Zusammenfassung für Q018

What help do you need most (from steward, manufacturer, regulators/authorities, sponsor companies, vulnerability program leaders, etc.) as a maintainer to make your project more attractive for your users, as they eventually may see CRA compliance as an adoption requirement?



Zusammenfassung für Q019

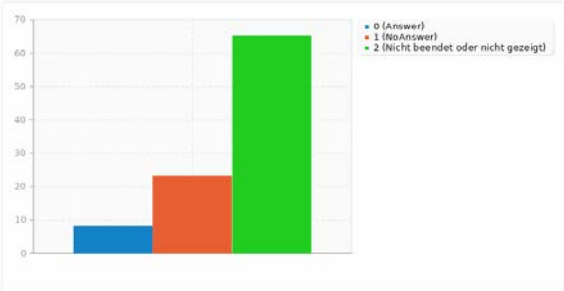
Are there any support services that you are already receiving and if so, what are they?

Antwort	Anzahl	Prozent
Antwort	8	8.33%
Keine Antwort	23	23.96%
Nicht beendet oder nicht gezeigt	65	67.71%

ID	Antwort
7	The only support that is meaningful is coming from the dev/other open source project community, not the manufacturer community.
54	No.
59	Voluntary code contributions.
60	No.
62	Open-collective
75	Main supporters for us are the Linux distributions, Ubuntu, Red Hat, SUSE, ... with their security teams, contributing vulnerability reports, patches/fixes, guidance on handling vulnerabilities, ...
82	No
86	No, just our own paid for legal counsel.

Zusammenfassung für Q019

Are there any support services that you are already receiving and if so, what are they?



Zusammenfassung für Q020

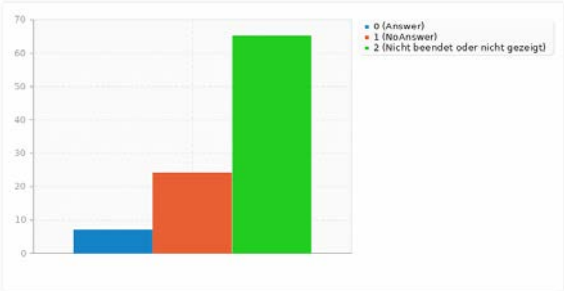
Who do you receive this support from?

Antwort	Anzahl	Prozent
Antwort	7	7.29%
Keine Antwort	24	25.00%
Nicht beendet oder nicht gezeigt	65	67.71%

ID	Antwort
7	The dev/committer community
59	Community members in the same position as I am.
60	N/A
62	One or two companies Interesses in our stuff - but close to nothing)
75	Security teams of Linux distributions.
82	N/A
86	Legal counsel.

Zusammenfassung für Q020

Who do you receive this support from?



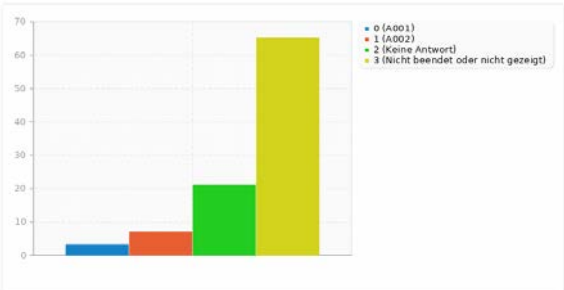
Zusammenfassung für Q021

Could this support already help you fulfil the CRA requirements?

Antwort	Anzahl	Prozent
yes (A001)	3	3.12%
no (A002)	7	7.29%
Keine Antwort	21	21.88%
Nicht beendet oder nicht gezeigt	65	67.71%

Zusammenfassung für Q021

Could this support already help you fulfil the CRA requirements?



Fragebogen für potentielle OSS Stewards in Bezug auf den CRA

Ergebnisse

Umfrage 415696

Anzahl der Datensätze in dieser Abfrage:	76
Gesamtzahl der Datensätze dieser Umfrage:	76
Anteil in Prozent:	100.00%

Zusammenfassung für Q00

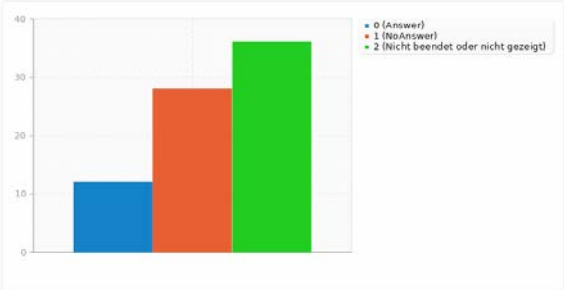
Was glaubt ihr, wodurch ihr zum Steward werdet?

Antwort	Anzahl	Prozent
Antwort	12	15.79%
Keine Antwort	28	36.84%
Nicht beendet oder nicht gezeigt	36	47.37%

ID	Antwort
57	Dadurch dass wir Open-Source-Projekte erstellen und anbieten.
60	durch tun (beitragen), darüber reden / lehren / unterrichten / Workshops geben
64	systematically providing support on a sustained basis for the development of the product.
65	Kommerzieller Support für OpenSource
66	Übernahme der Verantwortung für die langfristige Pflege eines Projekts.
74	Wie sind ein gemeinnütziger Verein, der sich um die Weiterentwicklung und Verbreitung einer FOSS kümmert.
95	Dadurch dass wir Open-Source-Projekte erstellen und anbieten.
98	durch tun (beitragen), darüber reden / lehren / unterrichten / Workshops geben
102	systematically providing support on a sustained basis for the development of the product.
103	Kommerzieller Support für OpenSource
104	Übernahme der Verantwortung für die langfristige Pflege eines Projekts.
112	Wie sind ein gemeinnütziger Verein, der sich um die Weiterentwicklung und Verbreitung einer FOSS kümmert.

Zusammenfassung für Q00

Was glaubt ihr, wodurch ihr zum Steward werdet?



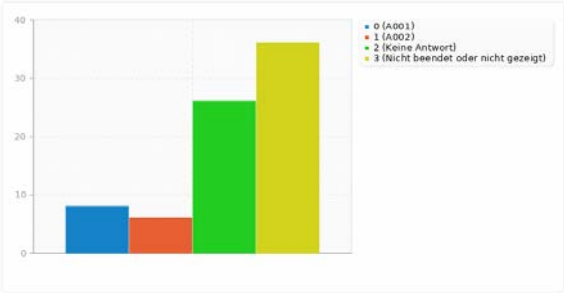
Zusammenfassung für Q001

Betrachten Sie sich als Hersteller und Steward, aber für unterschiedliche Projekte?

Antwort	Anzahl	Prozent
ja (A001)	8	10.53%
nein (A002)	6	7.89%
Keine Antwort	26	34.21%
Nicht beendet oder nicht gezeigt	36	47.37%

Zusammenfassung für Q001

Betrachten Sie sich als Hersteller und Steward, aber für unterschiedliche Projekte?



Zusammenfassung für Q002

Glauben Sie, dass Sie sich genauso leicht von der Rolle des Stewards zurücktreten können, wie diese anzunehmen?

Antwort	Anzahl	Prozent
ja (A001)	0	0.00%
nein (A002)	12	15.79%
Keine Antwort	28	36.84%
Nicht beendet oder nicht gezeigt	36	47.37%

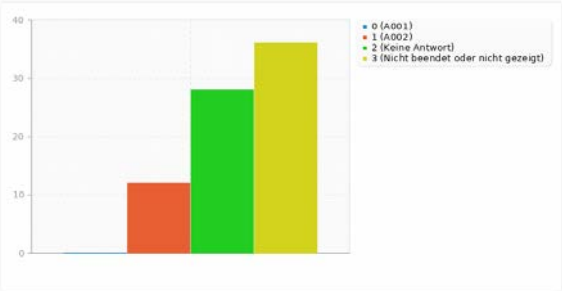
Zusammenfassung für Q003

Gibt es Vorgaben, bei denen du befürchtest, dass ihr sie als Steward nicht erfüllen könnt?

Antwort	Anzahl	Prozent
ja (A001)	6	7.89%
nein (A002)	6	7.89%
Keine Antwort	10	13.16%
Nicht beendet oder nicht gezeigt	54	71.05%

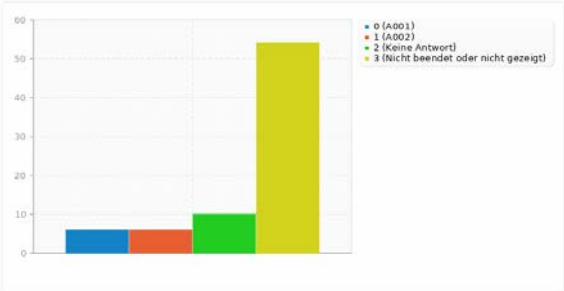
Zusammenfassung für Q002

Glauben Sie, dass Sie sich genauso leicht von der Rolle des Stewards zurücktreten können, wie diese anzunehmen?



Zusammenfassung für Q003

Gibt es Vorgaben, bei denen du befürchtest, dass ihr sie als Steward nicht erfüllen könnt?



Zusammenfassung für Q004

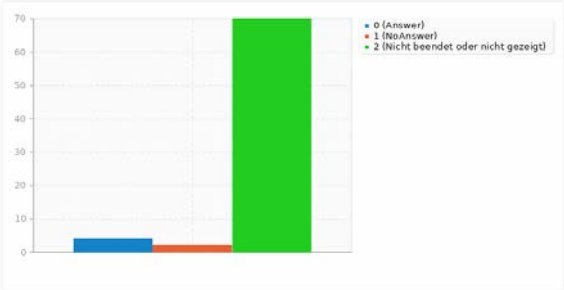
Welche sind das?

Antwort	Anzahl	Prozent
Antwort	4	5.26%
Keine Antwort	2	2.63%
Nicht beendet oder nicht gezeigt	70	92.11%

ID	Antwort
66	Zeitkritische Reaktion auf Schwachstellenmeldungen und die daraus folgenden Aktivitäten.
74	Generell stellt das CRA-Anforderungen, die wir noch nicht komplett erfüllen. Es ist absolut vorstellbar, dass wir die erfüllen, aber es werden trotzdem einmalig und dauerhaft zusätzliche Ressourcen benötigt werden, um das zu tun. Die sind ohnehin nicht gerade reichlich und einer ständigen Abwägung unterworfen. Es könnte also schwierig sein, die benötigten Ressourcen dauerhaft und regelmäßig zur Verfügung zu stellen. Beispiel Meldung von Schwachstellen: Wir haben ein freiwilliges Security-Team. Was passiert, wenn wir das nicht besetzt bekommen?
104	Zeitkritische Reaktion auf Schwachstellenmeldungen und die daraus folgenden Aktivitäten.
112	Generell stellt das CRA-Anforderungen, die wir noch nicht komplett erfüllen. Es ist absolut vorstellbar, dass wir die erfüllen, aber es werden trotzdem einmalig und dauerhaft zusätzliche Ressourcen benötigt werden, um das zu tun. Die sind ohnehin nicht gerade reichlich und einer ständigen Abwägung unterworfen. Es könnte also schwierig sein, die benötigten Ressourcen dauerhaft und regelmäßig zur Verfügung zu stellen. Beispiel Meldung von Schwachstellen: Wir haben ein freiwilliges Security-Team. Was passiert, wenn wir das nicht besetzt bekommen?

Zusammenfassung für Q004

Welche sind das?



Zusammenfassung für Q005

Habt ihr Befürchtungen vor etwaigen Konsequenzen, wenn Sie als Steward den Verpflichtungen der CRA nicht nachkommen?

Antwort	Anzahl	Prozent
ja (A001)	4	5.26%
nein (A002)	8	10.53%
Keine Antwort	10	13.16%
Nicht beendet oder nicht gezeigt	54	71.05%

Zusammenfassung für Q006

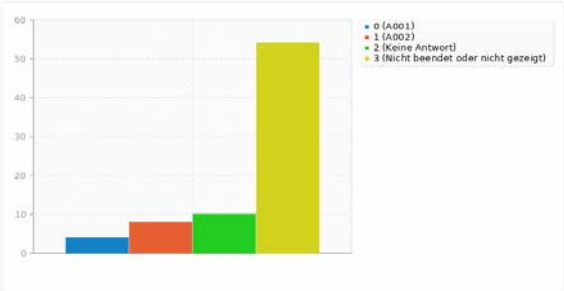
Welche sind das?

Antwort	Anzahl	Prozent
Antwort	2	2.63%
Keine Antwort	2	2.63%
Nicht beendet oder nicht gezeigt	72	94.74%

ID	Antwort
74	Vor allem Vertrauensverlust in die Software und oder Community.
112	Vor allem Vertrauensverlust in die Software und oder Community.

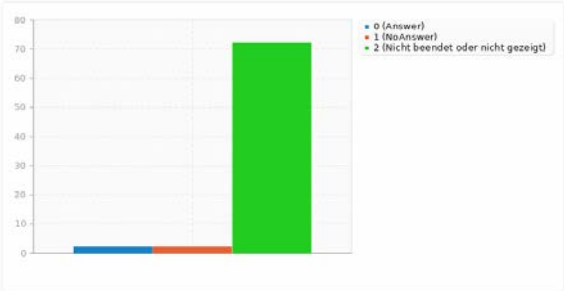
Zusammenfassung für Q005

Habt ihr Befürchtungen vor etwaigen Konsequenzen, wenn Sie als Steward den Verpflichtungen der CRA nicht nachkommen?



Zusammenfassung für Q006

Welche sind das?



Zusammenfassung für Q007

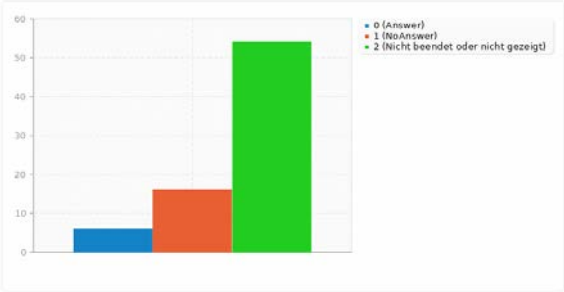
Was braucht ihr, um gegenüber den Herstellern nachzuweisen, dass die Open Source Komponenten die Anforderungen erfüllen?

Antwort	Anzahl	Prozent
Antwort	6	7.89%
Keine Antwort	16	21.05%
Nicht beendet oder nicht gezeigt	54	71.05%

ID	Antwort
60	Es muss klar, einfach & kurz sein - sonst haben zusätziiche Kriterienlisten keine Chance.
64	Ich fürchte dass gewisse Standards für die Projekte nicht zugänglich sein könnten Open source Projekte können nur Anforderungen erfüllen, welche ohne Kosten einsehbar sind.
66	Einen einfach ausfüllbaren Self-Assessment-Fragebogen mit entsprechenden Umsetzungshinweisen.
98	Es muss klar, einfach & kurz sein - sonst haben zusätziiche Kriterienlisten keine Chance.
102	Ich fürchte dass gewisse Standards für die Projekte nicht zugänglich sein könnten Open source Projekte können nur Anforderungen erfüllen, welche ohne Kosten einsehbar sind.
104	Einen einfach ausfüllbaren Self-Assessment-Fragebogen mit entsprechenden Umsetzungshinweisen.

Zusammenfassung für Q007

Was braucht ihr, um gegenüber den Herstellern nachzuweisen, dass die Open Source Komponenten die Anforderungen erfüllen?



Zusammenfassung für Q008

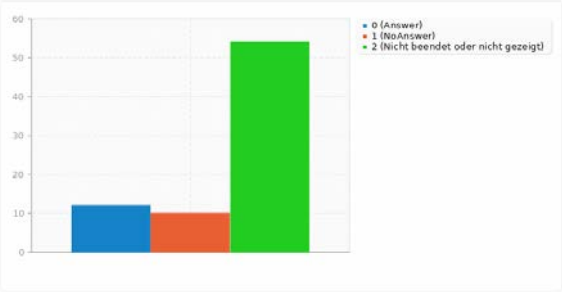
Wird es schwierig sein, die Anforderungen für die Meldung von Schwachstellen zu erfüllen (z. B. ENISA zu informieren)?

Antwort	Anzahl	Prozent
Antwort	12	15.79%
Keine Antwort	10	13.16%
Nicht beendet oder nicht gezeigt	54	71.05%

ID	Antwort
57	Nein
60	keine Ahnung.
64	Die der Inbetriebnahme der Reportingplatform und dem Inkrafttreten der Reportingpflichten scheint sehr kurz. Bitte die Platformen früher in (Test-)Betrieb nehmen!
65	Ja, der Kommunikationsaufwand kann groß sein (siehe curl)
66	Hierfür müssen entsprechende Prozesse und Tools etabliert werden.
74	Ja. S.o.
95	Nein
98	keine Ahnung.
102	Die der Inbetriebnahme der Reportingplatform und dem Inkrafttreten der Reportingpflichten scheint sehr kurz. Bitte die Platformen früher in (Test-)Betrieb nehmen!
103	Ja, der Kommunikationsaufwand kann groß sein (siehe curl)
104	Hierfür müssen entsprechende Prozesse und Tools etabliert werden.
112	Ja. S.o.

Zusammenfassung für Q008

Wird es schwierig sein, die Anforderungen für die Meldung von Schwachstellen zu erfüllen (z. B. ENISA zu informieren)?



Zusammenfassung für Q009

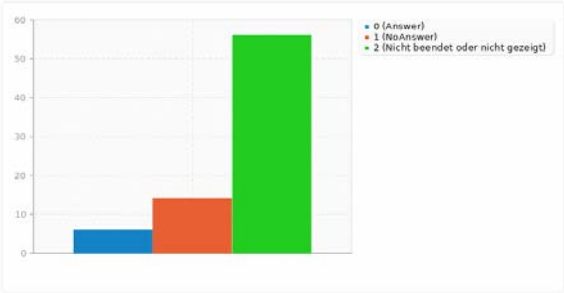
Was braucht ihr von den Open Source Entwicklern um die CRA Anforderungen zu erfüllen?

Antwort	Anzahl	Prozent
Antwort	6	7.89%
Keine Antwort	14	18.42%
Nicht beendet oder nicht gezeigt	56	73.68%

ID	Antwort
64	Müssen best practices bzgl. Entwicklungsprozess befolgen.
66	Dokumentation zur Struktur der Projekte
74	Das können wir aktuell noch nicht einschätzen.
102	Müssen best practices bzgl. Entwicklungsprozess befolgen.
104	Dokumentation zur Struktur der Projekte
112	Das können wir aktuell noch nicht einschätzen.

Zusammenfassung für Q009

Was braucht ihr von den Open Source Entwicklern um die CRA Anforderungen zu erfüllen?



Zusammenfassung für Q010

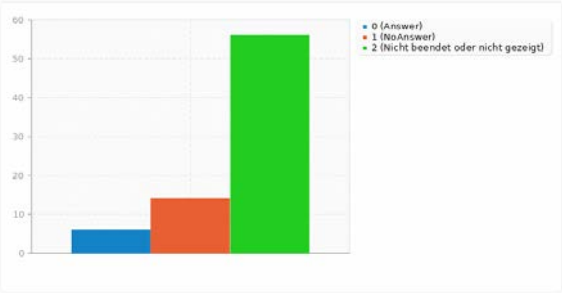
Was würden Sie in Betracht ziehen, wenn jemand Sie bittet, Steward zu werden?

Antwort	Anzahl	Prozent
Antwort	6	7.89%
Keine Antwort	14	18.42%
Nicht beendet oder nicht gezeigt	56	73.68%

ID	Antwort
65	Nur bei tragfähiger kommerzieller Grundlage.
66	Eine unabhängige Sicherheitsüberprüfung des Projekts sowie automatische Tools um neue Releases schnell prüfen zu können.
74	Wir können uns aktuell nicht vorstellen, dass das in Betracht kommt, wissen das also aktuell noch nicht.
103	Nur bei tragfähiger kommerzieller Grundlage.
104	Eine unabhängige Sicherheitsüberprüfung des Projekts sowie automatische Tools um neue Releases schnell prüfen zu können.
112	Wir können uns aktuell nicht vorstellen, dass das in Betracht kommt, wissen das also aktuell noch nicht.

Zusammenfassung für Q010

Was würden Sie in Betracht ziehen, wenn jemand Sie bittet, Steward zu werden?



Zusammenfassung für Q011

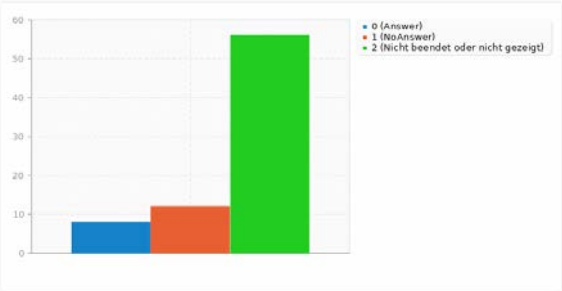
Für den Fall, dass es einen Nachweis gibt, der bescheinigt, dass eine Open Source Komponente die CRA Anforderungen erfüllt, ist die Bereitschaft da, als Steward für diese Geld zu erhalten (von den Herstellern), bzw. zu bezahlen (an Entwickler)?

Antwort	Anzahl	Prozent
Antwort	8	10.53%
Keine Antwort	12	15.79%
Nicht beendet oder nicht gezeigt	56	73.68%

ID	Antwort
64	Eventuell Oma geringen Maße.
65	ja
66	Ja
74	Ja, das entspricht auch aktuell schon in Teilen unserer Vorgehensweise.
102	Eventuell Oma geringen Maße.
103	ja
104	Ja
112	Ja, das entspricht auch aktuell schon in Teilen unserer Vorgehensweise.

Zusammenfassung für Q011

Für den Fall, dass es einen Nachweis gibt, der bescheinigt, dass eine Open Source Komponente die CRA Anforderungen erfüllt, ist die Bereitschaft da, als Steward für diese Geld zu erhalten (von den Herstellern), bzw. zu bezahlen (an Entwickler)?



Zusammenfassung für Q012

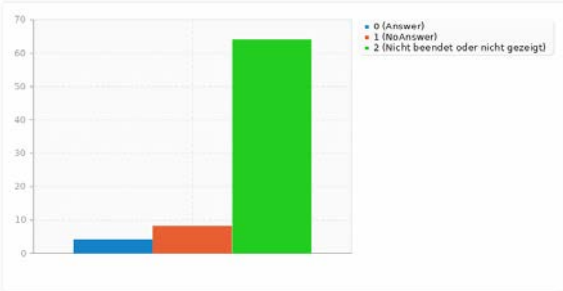
Welche Unterstützung benötigen Sie außerdem (von Herstellern, Aufsichtsbehörden, Sponsoren, Leitern von Schwachstellenprogrammen usw.), um die Anforderungen des CRA zu erfüllen?

Antwort	Anzahl	Prozent
Antwort	4	5.26%
Keine Antwort	8	10.53%
Nicht beendet oder nicht gezeigt	64	84.21%

ID	Antwort
65	Faire Entlohnung für die Aufwände
66	Tooling, um die Sicherheit von Projekt-Updates schnell prüfen zu können. Eine Haftpflichtversicherung, die gegenüber dem Hersteller die Risiken übernehmen kann.
103	Faire Entlohnung für die Aufwände
104	Tooling, um die Sicherheit von Projekt-Updates schnell prüfen zu können. Eine Haftpflichtversicherung, die gegenüber dem Hersteller die Risiken übernehmen kann.

Zusammenfassung für Q012

Welche Unterstützung benötigen Sie außerdem (von Herstellern, Aufsichtsbehörden, Sponsoren, Leitern von Schwachstellenprogrammen usw.), um die Anforderungen des CRA zu erfüllen?



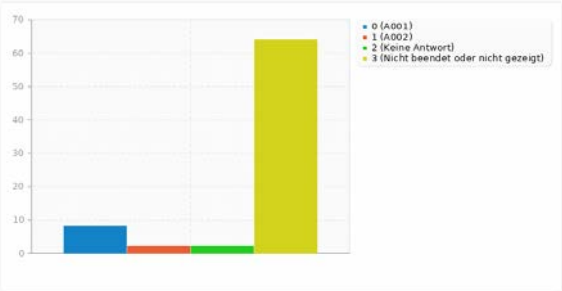
Zusammenfassung für Q013

Sind Sie der Meinung, dass Hersteller Stewards unterstützen müssen?

Antwort	Anzahl	Prozent
ja (A001)	8	10.53%
nein (A002)	2	2.63%
Keine Antwort	2	2.63%
Nicht beendet oder nicht gezeigt	64	84.21%

Zusammenfassung für Q013

Sind Sie der Meinung, dass Hersteller Stewards unterstützen müssen?



Questionnaire for potential OSS Stewards in terms of CRA

Ergebnisse

Umfrage 146965

Anzahl der Datensätze in dieser Abfrage:	53
Gesamtzahl der Datensätze dieser Umfrage:	53
Anteil in Prozent:	100.00%

Zusammenfassung für Q00

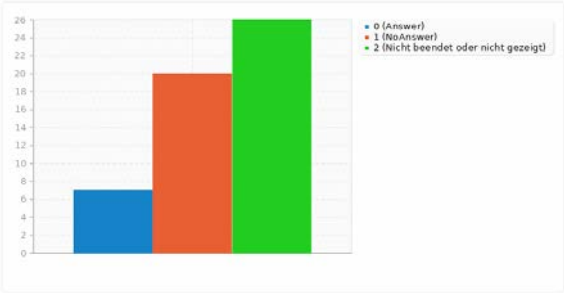
What do you think makes you a steward?

Antwort	Anzahl	Prozent
Antwort	7	13.21%
Keine Antwort	20	37.74%
Nicht beendet oder nicht gezeigt	26	49.06%

ID	Antwort
3	20 years of experience enhancing, debugging, and maintaining multiple open source projects.
4	My conpany creates free/open source software (F/OSS).
7	Our foundation, Stichting Trifecta Tech Foundation, is a non-profit and public benefit organization ("ANBI" in the Netherlands). We build and maintain libraries and utilities that are used by others in commercial and non-commercial products, such as other libraries, open-source operating systems and commercial end-user products.
18	From hearsay, possibly a steward
31	We are a non-profit promoting Open Source software and thinking about becoming a steward for the software created in our field.
32	I have been maintaining and using FOSS for years.
43	We are in charge of an open source solution Project.

Zusammenfassung für Q00

What do you think makes you a steward?



Zusammenfassung für Q009

Do you consider yourself a Manufacturer and a Steward , but for different projects?

Antwort	Anzahl	Prozent
yes (A001)	3	5.66%
no (A002)	6	11.32%
Keine Antwort	18	33.96%
Nicht beendet oder nicht gezeigt	26	49.06%

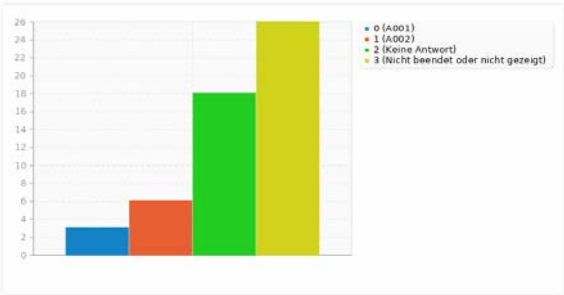
Zusammenfassung für Q010

Do you think you can as easily opt-out from as opt-in for the Steward role?

Antwort	Anzahl	Prozent
yes (A001)	2	3.77%
no (A002)	4	7.55%
Keine Antwort	21	39.62%
Nicht beendet oder nicht gezeigt	26	49.06%

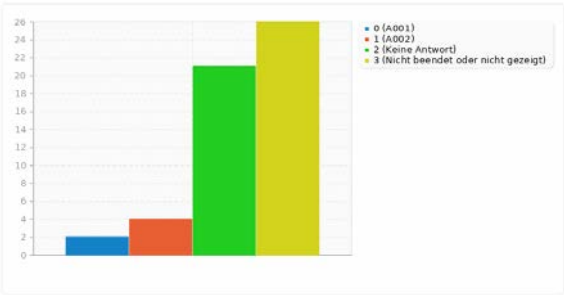
Zusammenfassung für Q009

Do you consider yourself a Manufacturer and a Steward , but for different projects?



Zusammenfassung für Q010

Do you think you can as easily opt-out from as opt-in for the Steward role?



Zusammenfassung für Q001

Are there any requirements that you fear you will not be able to fulfil as a steward?

Antwort	Anzahl	Prozent
yes (A001)	4	7.55%
no (A002)	3	5.66%
Keine Antwort	11	20.75%
Nicht beendet oder nicht gezeigt	35	66.04%

Zusammenfassung für Q012

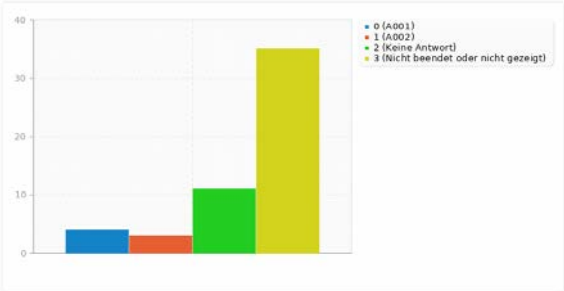
What are these?

Antwort	Anzahl	Prozent
Antwort	2	3.77%
Keine Antwort	2	3.77%
Nicht beendet oder nicht gezeigt	49	92.45%

ID	Antwort
31	All of them. There is no funding yet, so that needs to come from somewhere.
43	The CRA unrealistic perfection goals

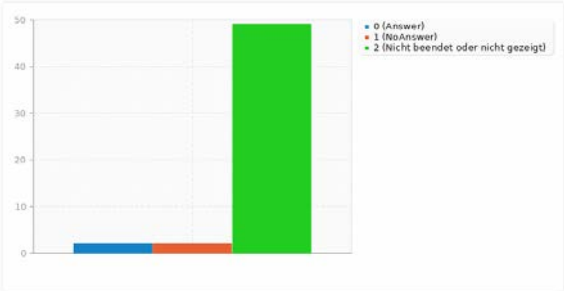
Zusammenfassung für Q001

Are there any requirements that you fear you will not be able to fulfil as a steward?



Zusammenfassung für Q012

What are these?



Zusammenfassung für Q002

Are you afraid of any consequences if you as a steward don't meet CRA obligations?

Antwort	Anzahl	Prozent
yes (A001)	4	7.55%
no (A002)	3	5.66%
Keine Antwort	11	20.75%
Nicht beendet oder nicht gezeigt	35	66.04%

Zusammenfassung für Q013

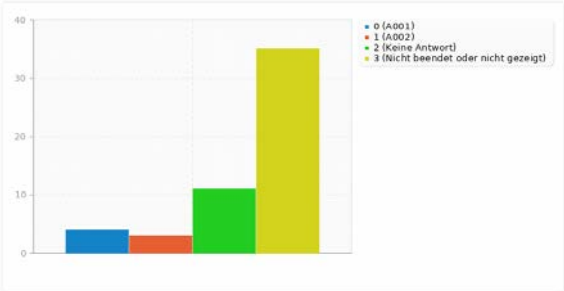
What are these?

Antwort	Anzahl	Prozent
Antwort	2	3.77%
Keine Antwort	2	3.77%
Nicht beendet oder nicht gezeigt	49	92.45%

ID	Antwort
3	Newly discovered vulnerabilities that only I or others on the dev team can properly/timely fix...with no support from consumers (manufacturers and other downstream projects).
44	not supporting correctly our community

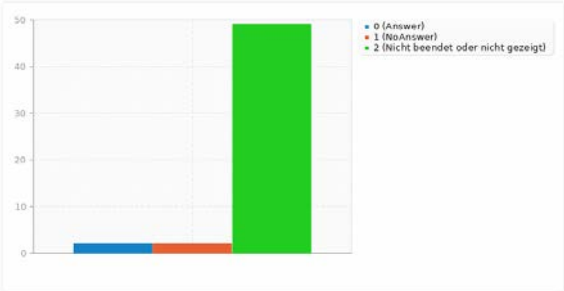
Zusammenfassung für Q002

Are you afraid of any consequences if you as a steward don't meet CRA obligations?



Zusammenfassung für Q013

What are these?



Zusammenfassung für Q003

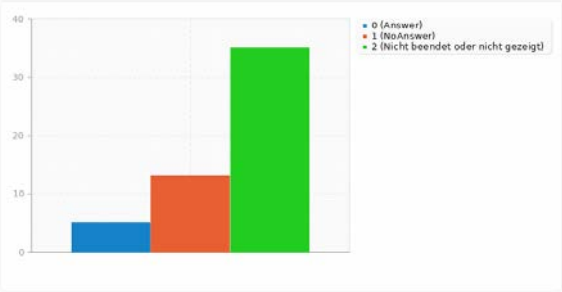
What do you need to prove to the manufacturers that the open-source components fulfil the requirements?

Antwort	Anzahl	Prozent
Antwort	5	9.43%
Keine Antwort	13	24.53%
Nicht beendet oder nicht gezeigt	35	66.04%

ID	Antwort
1	That's up to the manufacturers to determine, not the steward.
3	That's a silly question. The 'requirements' are always that the open source software (especially infrastructure software/libs/middleware/etc) be 'secure' by today's definition. Such requirements can never be actually met by the authors/technical people. It always requires both maintenance and innovation (e.g. quantum crypto). So, the question actually is: how do you support the innovation and maintenance needs of the software consumers...without them doing it themselves? First, they can't do it themselves...no matter what their 'requirements'. You might be able to fool the manufacturers that the open source components fulfill their requirements, it will be a big surprise to them when their 'requirements' for bug-free/secure software are no longer met.
18	Afaict there's no such obligation for stewards to *prove* anything to manufacturers.
31	We'll need SBOMs, that's clear. But everything else is quite unclear. So the short answer ist: We don't know yet.
43	Sbon I suppose

Zusammenfassung für Q003

What do you need to prove to the manufacturers that the open-source components fulfil the requirements?



Zusammenfassung für Q011

Will it be hard to comply with vulnerability notification requirements (e.g, notify ENISA)?

Antwort	Anzahl	Prozent
yes (A001)	3	5.66%
no (A002)	4	7.55%
Keine Antwort	11	20.75%
Nicht beendet oder nicht gezeigt	35	66.04%

Zusammenfassung für Q004

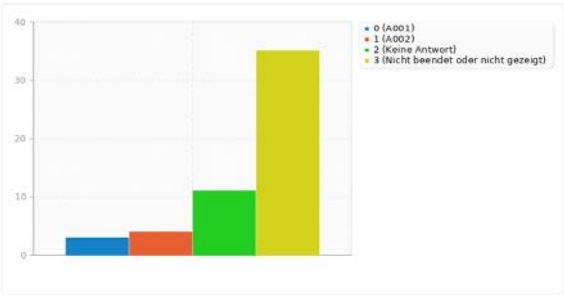
What do you need from the open-source developers to fulfil the CRA requirements?

Antwort	Anzahl	Prozent
Antwort	5	9.43%
Keine Antwort	9	16.98%
Nicht beendet oder nicht gezeigt	39	73.58%

ID	Antwort
1	Nothing
3	From the perspective of an open source developer, my realistic expectation is that consumers are happy to get everything from open source (innovation, security, reliability, etc., etc) for nothing all. Further, they will frequently expect thanks from the project team for them using the open source software in their product that they charge their consumers for. This is defective and can't be sustained.
18	No idea
31	The question is not: What do we need. The question is: What can we provide them with. Until we help the developers, the whole thing will not fly.
43	The Framework to offer Support contracts.

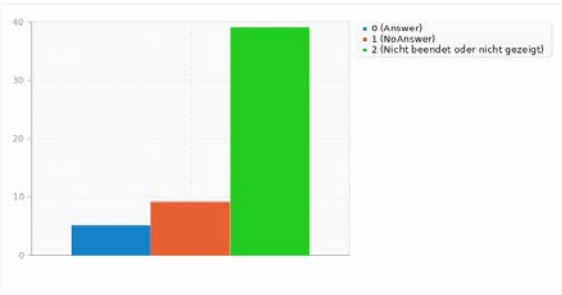
Zusammenfassung für Q011

Will it be hard to comply with vulnerability notification requirements (e.g, notify ENISA)?



Zusammenfassung für Q004

What do you need from the open-source developers to fulfil the CRA requirements?



Zusammenfassung für Q005

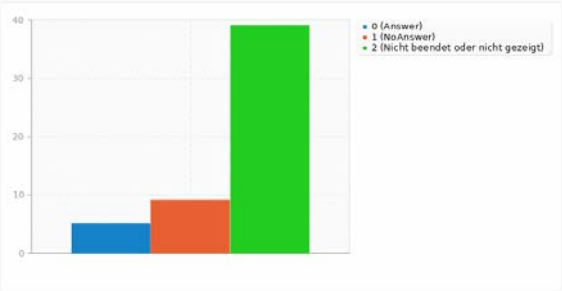
What would you consider if somebody asks you to become a steward?

Antwort	Anzahl	Prozent
Antwort	5	9.43%
Keine Antwort	9	16.98%
Nicht beendet oder nicht gezeigt	39	73.58%

ID	Antwort
1	N/A
3	I'd ask myself: do I really know enough about this software to be able to maintain it? What if someone had asked me to fix the log4j bug? Could I have done it in a day? If not, who could have?
18	If becoming a steward is not an obligation that follows from CRA, I'd try to avoid it
31	We'll have to find funding first. If we can find that, yes, we'll consider it.
43	?

Zusammenfassung für Q005

What would you consider if somebody asks you to become a steward?



Zusammenfassung für Q006

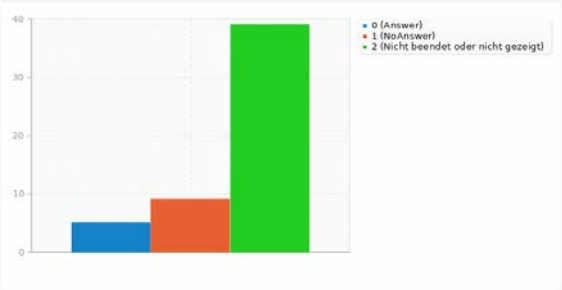
In the event that there is proof that an open-source component fulfils the CRA requirements, is there a willingness to receive money for this as a steward (from the manufacturers) or to pay for it (to developers)?

Antwort	Anzahl	Prozent
Antwort	5	9.43%
Keine Antwort	9	16.98%
Nicht beendet oder nicht gezeigt	39	73.58%

ID	Antwort
1	Payment is not part of the CRA at all, please do not conflate it with proper support of open source projects by community members and companies.
3	As per above, talking about fulfilling static 'security requirements' is silly. It just doesn't match reality. I'm sure, however, that there will be plenty of people that will say 'yes' to willingness to receive money...but not be able to actually maintain or innovate around a given projects (see answer to previous question).
18	Whatever helps to build a healthy Open Source ecosystem
31	Yes, I believe the willingness is there in our organization. But this comes with a lot of overhead that needs to be paid for and so far there is no indication that the manufacturers are willing to pay for that. It is unclear how to business model for the steward is going to work. In order to have something to sell, we'd probably have to give this "proof" only to paying manufacturers?
43	That is Not the point

Zusammenfassung für Q006

In the event that there is proof that an open-source component fulfils the CRA requirements, is there a willingness to receive money for this as a steward (from the manufacturers) or to pay for it (to developers)?



Zusammenfassung für Q007

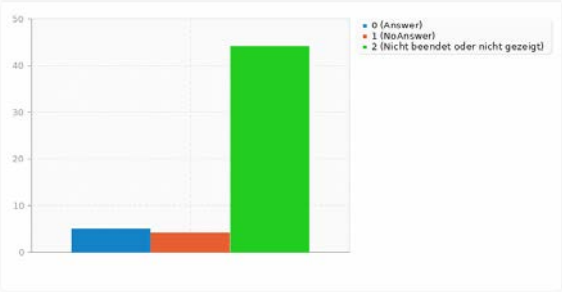
What help do you need (from manufacturer, regulators/authorities, sponsor companies, vulnerability program leaders, etc.) to fulfil CRA requirements?

Antwort	Anzahl	Prozent
Antwort	5	9.43%
Keine Antwort	4	7.55%
Nicht beendet oder nicht gezeigt	44	83.02%

ID	Antwort
1	Send security bug reports to the documented contact points, ideally with proposed fixes for those reported security issues.
3	From manufacturers (consumers of project software): Support (money and/or appropriately skilled people). From regulators: A sustainable, reality-based policy that provides for a maintenance-support-system that works in the real world (where only a few people can serve as stewards for a given open source project).
18	Explain CRA requirements to affected software developers
31	From regulator/authorities: Clear guidance on many open questions. From somebody: Money to pay for overhead and development. From somebody: Better tools for SBOM management and other organizational issues.
43	I do need an active role of authorities to tackle vulnerabilities by their own actions.

Zusammenfassung für Q007

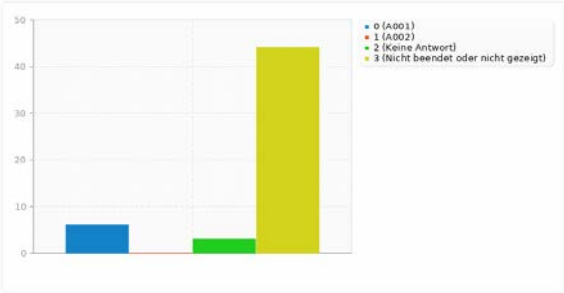
What help do you need (from manufacturer, regulators/authorities, sponsor companies, vulnerability program leaders, etc.) to fulfil CRA requirements?



Zusammenfassung für Q008

Do you think manufacturers must support stewards?

Antwort	Anzahl	Prozent
yes (A001)	6	11.32%
no (A002)	0	0.00%
Keine Antwort	3	5.66%
Nicht beendet oder nicht gezeigt	44	83.02%

Zusammenfassung für Q008

Do you think manufacturers must support stewards?