**OpenChain Specification**

Version 2.0

* Translation Draft Englisch / Deutsch –

Establishing trust in the Open Source from which Software Solutions are built

Vertrauen in Open Source schaffen, aus welcher Softwarelösungen entstehen

Inhaltsverzeichnis

Copyright © 2016-2019 Linux Foundation. Dieses Dokument ist unter der Creative Commons Attribution 4.0 International (CC-BY 4.0) Lizenz lizenziert. Eine Kopie des Lizenztexts finden Sie unter https://creativecommons.org/licenses/by/4.0/.

1. Einleitung

|  |  |
| --- | --- |
| DRAFT OCSpec 2.0 final Draft  09.04.2019 | Draft deutsche Übersetzung |
| This specification defines the key requirements of a quality open source license compliance program. The objective is to provide a benchmark that builds trust between organizations exchanging software solutions comprised of open source software. Specification conformance provides assurance that a Program has been designed to produce the required Compliance Artifacts (i.e., legal notices, source code and so forth) for each software solution. The OpenChain Specification focuses on the “what” and “why” aspects of a Program rather than the “how” and “when”. This ensures flexibility for different organizations of different sizes in different markets to choose specific policy and process content that fits their size, goals and scope. For instance, an OpenChain Conformant Program may address a single product line or the entire organization.  This introduction provides the context for all potential users. Section 2 defines key terms used throughout the Specification. Section 3 defines the requirements that a Program must satisfy to achieve conformance. A requirement consists of one or more Verification Materials (i.e., records) that must be produced to satisfy the requirement. Verification Materials are not required to be made public, though an organization may choose to provide them to others, potentially under a Non-Disclosure Agreement (NDA).  The Specification is developed as an open initiative with feedback received from over 150 contributors. Insight into its historical development can be obtained by reviewing the Specification [mailing list](https://lists.linuxfoundation.org/mailman/listinfo/openchain-spec) and [Frequently Asked Questions (FAQs).](https://wiki.linuxfoundation.org/openchain/specification-questions-and-answers) | Die vorliegende Spezifikation definiert die Schlüsselanforderungen an ein qualitätsgesichertes Open-Source-Lizenz-Compliance-Programm. Sie zielt darauf ab, eine Benchmark bereitzustellen, welche zwischen Unternehmen Vertrauen beim Austausch von Open-Source-Software beinhaltenden Softwarelösungen schafft. Das Einhalten der Spezifikation liefert den Nachweis dafür, dass ein Programm geschaffen wurde, um die erforderlichen Compliance-Artefakte (d.h. Rechtsinhalte, Quellcode, usw.) für jede Softwarelösung zu erzeugen. Die OpenChain-Spezifikation konzentriert sich auf die "Was" und "Warum" -Beschaffenheit eines Programms, anstatt "Wie" und "Wenn" -Überlegungen anzustellen. Dies sichert unterschiedlichen Unternehmen mit unterschiedlicher Größe in unterschiedlichen Märkten die Flexibilität, diejenigen Richtlinien und Prozesse auszuwählen, die auf ihre Größe, ihre Ziele und ihren Anwendungsbereich zugeschnitten sind. So kann bspw. ein OpenChain-konformes Programm sich auf ein einzelnes Produkt oder aber das gesamte Unternehmen beziehen.  Die vorliegende Einführung liefert allen potentiellen Nutzern den Kontext. Abschnitt 2 definiert Schlüsselbegriffe, die in der Spezifikation genutzt werden. Abschnitt 3 bestimmt die Anforderungen, die ein Programm erfüllen muss, um Konformität zu erreichen. Jeder Anforderung ist eine Liste von Verifikationsmaterial (d.h. Nachweisen) zugeordnet, welches vorhanden sein muss, damit eine bestimmte Anforderung als erfüllt angesehen werden kann. Verifikationsmaterial muss nicht veröffentlicht werden, wenngleich ein Unternehmen sich dazu entschließen kann, dieses Dritten zugänglich zu machen – bspw. nach Abschluss einer Geheimhaltungsvereinbarung (Non-Disclosure Agreement bzw. NDA).  Die Spezifikation wurde in einer offenen Initiative entwickelt, in welche Beiträge von mehr als 150 Mitwirkenden eingeflossen sind. Einen Einblick in die Entwicklungsgeschichte erhalten Sie über die [Spezifikations-Mailingliste](https://lists.linuxfoundation.org/mailman/listinfo/openchain-spec) und in den [häufig gestellten Fragen (FAQs)](https://wiki.linuxfoundation.org/openchain/specification-questions-and-answers). |

1. Definitionen

|  |  |
| --- | --- |
| “**Compliance Artifacts**”- a collection of artifacts that represent the output of the Program for the Supplied Software. The collection may include (but is not limited to) one or more of the following: source code, attribution notices, copyright notices, copy of licenses, modification notifications, written offers, Open Source component bill of materials, and SPDX documents.  “**Identified Licenses**”- a set of Open Source Software licenses identified as a result of following an appropriate method of identifying Open Source components from which the Supplied Software is comprised.  “**OpenChain Conformant**” - a Program that satisfies all the requirements of this specification.  “**Open Source**”- software subject to one or more licenses that meet the Open Source Definition published by the Open Source Initiative (OpenSource.org) or the Free Software Definition (published by the Free Software Foundation) or similar license.  “**Program**” – the set of policies, processes and personnel that manage an organization’s Open Source license compliance activities.  “**Software Staff**” - any organization employee or contractor that defines, contributes to or has responsibility for preparing Supplied Software. Depending on the organization, that may include (but is not limited to) software developers, release engineers, quality engineers, product marketing and product management.  “**SPDX**” - the format standard created by the Linux Foundation’s SPDX (Software Package Data Exchange) Working Group for exchanging license and copyright information for a given software package. A description of the SPDX specification can be found at [www.spdx.org](http://www.spdx.org).  “**Supplied Software**”- software that an organization distributes to third parties (e.g., other organizations or individuals).  “**Verification Materials**” - materials that demonstrate that a given requirement is satisfied. | **„Compliance-Artefakte“ –** Eine Zusammenstellung von Artefakten, die das Ergebnis des Programms für eine Zugelieferte Software darstellt.  Die Zusammenstellung kann eines oder mehrere der folgenden Elemente enthalten (ist aber nicht auf diese beschränkt): Quellcode, Benennung des Autors, Urheberrechtshinweise, Kopien der Lizenzbedingungen, Bearbeitungshinweise, schriftliche Angebote, eine Open-Source-Komponenten-Stückliste („Bill of Materials“ bzw. „BoM"), SPDX-Dokumente, etc.  **„Identifizierte Lizenzen“** – eine Reihe von Open-Source-Softwarelizenzen, identifiziert als Ergebnis einer geeigneten Methode zur Identifizierung derjenigen Open-Source-Komponenten, aus denen sich eine Zugelieferte Software zusammensetzt.  **„OpenChain-konform“** – ein Programm, das alle Anforderungen dieser Spezifikation erfüllt.  **„Open Source“** - Software, die einer oder mehreren Lizenzen unterliegt, die den Definitionsanforderungen für Open Source der Open Source Initiative (OpenSource.org), denen für Freie Software (veröffentlicht durch die Free Software Foundation) oder einer ähnlichen Lizenz entsprechen.  **„Programm“** – Richtlinien, Prozesse und Mitarbeiter, die die Compliance-Aktivitäten eines Unternehmensfür Open Source-Lizenzen steuern.  **„Software-Mitarbeiter“** - jeder Mitarbeiter oder Auftragnehmer eines Unternehmens, der die Vorgaben für Zugelieferte Software festlegt, zu ihr beiträgt oder für ihre Vorbereitung verantwortlich ist. Abhängig vom jeweiligen Unternehmen können dies insbesondere (und nicht nur) Software-Entwickler, Release-Ingenieure, Qualitätsprüfer, sowie Mitarbeiter im Produkt-Marketing und im Produkt-Management sein.  **„SPDX“** - der von der SPDX (Software Package Data Exchange)-Arbeitsgruppe der Linux Foundation erstellte Format-Standard für den Austausch von Lizenz- und Urheberrechtsinformationen für ein bestimmtes Softwarepaket. Eine Beschreibung der SPDX-Spezifikation finden Sie unter [www.spdx.org](http://www.spdx.org).  **„Zugelieferte Software“** - Software, welche ein Unternehmen an Dritte weitergibt (z. B. andere Unternehmen oder Einzelpersonen).  **„Verifikationsmaterial“** - Nachweise, die vorhanden sein müssen, damit eine bestimmte Anforderung als erfüllt angesehen werden kann. |

3) Anforderungen

|  |  |
| --- | --- |
| 1.0 Program Foundation | 1.0 Programm-Grundlagen |
| **1.1 Policy**  A written Open Source policy exists that governs Open Source license compliance of the Supplied Software. The policy must be internally communicated.  **Verification Material(s):**  1.1.1 A documented Open Source policy.  1.1.2 A documented procedure that makes Software Staff aware of the existence of the Open Source policy (e.g., via training, internal wiki, or other practical communication method).  **Rationale:**  To ensure steps are taken to create, record and make Software Staff aware of the existence of an Open Source policy. Although no requirements are provided here on what should be included in the policy, other sections may impose requirements on the policy.  1.2 Competence  The organization shall:   * Identify the roles and the corresponding responsibilities of those roles that affects the performance and effectiveness of the Program; * Determine the necessary competence of person(s) fulfilling each role * Ensure that these persons are competent on the basis of appropriate education, training, and/or experience; * Where applicable, take actions to acquire the necessary competence; and * Retain appropriate documented information as evidence of competence.   **Verification Material(s):**  1.2.1 A documented list of roles with corresponding responsibilities for the different participants in the Program.  1.2.2 A document that identifies the competencies for each role.  1.2.3 Documented evidence of assessed competence for each Program participant.  **Rationale:**  To ensure that the identified participants fulfilling Program roles have obtained a sufficient level of competence for their respective roles and responsibilities.  1.3 Awareness  The organization shall ensure that Program participants are aware of:  a) The Open Source policy;  b) Relevant Open Source objectives;  c) Their contribution to the effectiveness of the Program; and  d) The implications of not following the Program’s requirements.  Verification Material(s):  1.3.1Documented evidence of assessed awareness for each Program personnel including the Program’s objectives, ones contribution within the Program, and implications of Program non-conformance.  Rationale:  To ensure Program personnel have obtained a sufficient level of awareness for their respective roles and responsibilities within the Program.  1.4 Program Scope  Different Programs may be governed by different levels of scope. For example, a program could govern a single product line, an entire department or an entire organization. The scope designation needs to be declared for each Program.  Verification Material(s):  1.4.1 A written statement that clearly defines the scope and limits of the Program.  Rationale:  To provide the flexibility to construct a Program that best fits the scope of an organization’s needs. Some organizations could choose to maintain a Program for a specific product line while others could implement a Program to govern the Supplied Software of the entire organization.  1.5 License Obligations  A process exists for reviewing the Identified Licenses to determine the obligations, restrictions and rights granted by each license.  Verification Material(s):  1.5.1 A documented procedure to review and document the obligations, restrictions and rights granted by each Identified License.  Rationale:  To ensure a process exists for reviewing and identifying the license obligations for each Identified License for the various use cases an organization may encounter (as defined in requirement 3.2). | 1.1 Richtlinie  Es existiert eine schriftliche Open-Source-Richtlinie, in der die Anforderungen an die Open-Source-Lizenz-Compliance der Zugelieferten Software geregelt ist. Die Richtlinie muss innerhalb des Unternehmens kommuniziert werden.  Verifikationsmaterial:  1.1.1 Eine schriftlich dokumentierte Open-Source-Richtlinie.  1.1.2 Ein dokumentiertes Verfahren, welches die Software-Mitarbeiter auf die Existenz der Open-Source-Richtlinie aufmerksam macht (z. B. über Schulungen, ein internes Wiki oder eine andere gängige Kommunikationsmethode).  Begründung:  Es soll sichergestellt werden, dass die notwendigen Schritte unternommen wurden, um eine Open-Source-Richtlinie zu erstellen, festzulegen und Software-Mitarbeiter auf deren Existenz hinzuweisen. Obwohl an dieser Stelle keine inhaltlichen Vorgaben an die Open-Source-Richtlinie gestellt werden, können diese durch andere Abschnitte dieser Spezifikation auferlegt werden.  1.2 (Fach-)Kompetenz  Das Unternehmen muss:   * Diejenigen Rollen und zugehörigen Verantwortlichkeiten dieser Rollen identifizieren, die die Performanz und Effektivität des Programms beeinflussen. * Den notwendigen Grad an Fachkompetenz der Person(en) bestimmen, welche die jeweilige Rolle bekleiden * Sicherstellen, dass diese Personen auf Basis einschlägiger Ausbildung, Schulung und/oder Erfahrung die notwendige Fachkompetenz besitzen * Falls notwendig: Maßnahmen ergreifen, dass die hinreichende Fachkompetenz erworben wird; und * Eine hinreichende Dokumentation als Beleg der Fachkompetenz aufrechterhalten.   Verifikationsmaterial:  1.2.1 Eine dokumentierte Liste an Rollen inklusive zugehöriger Verantwortlichkeiten für die unterschiedlichen Programmteilnehmer.  1.2.2 Ein Dokument, welches die Kompetenzanforderungen an die jeweiligen Rollen festlegt.  1.2.3 Dokumentierte Nachweise der bei jedem Programm-Teilnehmer ermittelten Fachkompetenz.  Begründung:  Es soll sichergestellt werden, dass diejenigen Teilnehmer, welche Rollen im Programm ausführen, einen der jeweiligen Rolle und Verantwortlichkeit angemessenen Grad an Fachkompetenz erreicht haben.  1.3. Bekanntheit  Das Unternehmen muss sicherstellen, dass Programm-Teilnehmern   1. die Open-Source-Richtlinie; 2. relevante Open-Source-Ziele; 3. ihr jeweiliger Beitrag zur Effektivität des Open-Source-Compliance-Programms; 4. die Auswirkungen einer Nichterfüllung der Programm-Anforderungen   bekannt sind.  Verifikationsmaterial:  1.3.1 Dokumentierte Nachweise des bei jedem Programm-Teilnehmer ermittelten Bekanntheitsgrades in Bezug auf die Programmziele, ihren jeweiligen Beitrag zum Programm und der Auswirkungen einer Nichtkonformität gegenüber dem Programm.  Begründung:  Es soll sichergestellt werden, dass den Teilnehmern ihre jeweiligen Rollen und Verantwortlichkeiten innerhalb des Programms in hinreichendem Maße bekannt sind.  1.4 Programmumfang  Für unterschiedliche Programme gelten möglicherweise unterschiedliche Definitionen zu deren Umfang. Beispielsweise könnte ein Programm sich auf eine einzelne Produktlinie, einen Unternehmensbereich oder ein gesamtes Unternehmen beziehen. Für jedes Programm muss der Umfang festgelegt werden.  Verifikationsmaterial:  1.4.1 Eine schriftliche Erklärung, welche Umfang und Grenzen des Programms klar definiert.  Begründung:  Es soll sichergestellt werden, dass die Flexibilität besteht, ein Programm aufzusetzen, welches den Anforderungen eines Unternehmens am besten entspricht. Einige Unternehmen könnten ein Programm für eine bestimmte Produktlinie unterhalten, während andere ein Programm zur Steuerung der Zugelieferten Software des gesamten Unternehmens einrichten könnten.  1.5 Lizenzverpflichtungen  Es besteht ein Verfahren zur Überprüfung der Identifizierten Lizenzen um jeweils gewährte Rechte bzw. auferlegte Einschränkungen und Verpflichtungen zu bestimmen.  Verifikationsmaterial:  1.5.1 Ein dokumentiertes Verfahren zur Überprüfung und Dokumentation der durch die jeweiligen Identifizierten Lizenzen gewährten Rechte bzw. auferlegten Beschränkungen und Verpflichtungen.  Begründung:  Es soll sichergestellt werden, dass ein Prozess besteht, in dem die Lizenzpflichten für die verschiedenen, im Kontext des Unternehmens möglichen, Anwendungsfälle geprüft und identifiziert werden (wie in Anforderung 3.2 definiert). |

|  |  |
| --- | --- |
| 2.0 Relevant Tasks Defined and Supported | 2.0 Definition und Unterstützung relevanter Aufgaben |
| 2.1 Access  Maintain a process to effectively respond to external Open Source inquiries. Publicly identify a means by which a third party can make an Open Source compliance inquiry.  Verification Material(s):  2.1.1 Publicly visible method that allows any third party to make an Open Source license compliance inquiry (e.g., via a published contact email address, or the Linux Foundation's Open Compliance Directory).  2.1.2 An internal documented procedure for responding to third party Open Source license compliance inquiries.  Rationale:  To ensure there is a reasonable way for third parties to contact the organization with regard to Open Source compliance inquiries and that the organization is prepared to effectively respond.  2.2 Effectively Resourced  Identify and Resource Program Task(s):   * Assign accountability to ensure the successful execution of Program tasks. * Program tasks are sufficiently resourced:   + Time to perform the tasks have been allocated; and   + Adequate funding has been allocated. * A process exists for reviewing and updating the policy and supporting tasks; * Legal expertise pertaining to Open Source license compliance is accessible to those who may need such guidance; and * A process exists for the resolution of Open Source license compliance issues.   Verification Material(s):  2.2.1 Document with name of persons, group or function in Program role(s)identified.  2.2.2 The identified Program roles have been properly staffed and adequate funding provided.  2.2.3 Identification of legal expertise available to address Open Source license compliance matters which could be internal or external.  2.2.4 A documented procedure that assigns internal responsibilities for Open Source compliance.  2.2.5 A documented procedure for handling the review and remediation of non-compliant cases.  Rationale:  To ensure: i) Program responsibilities are effectively supported and resourced and ii) policies and supporting processes are regularly updated to accommodate changes in Open Source compliance best practices. | 2.1 Zugang  Erstellung und Aufrechterhaltung eines Prozesses, um auf Open-Source-Anfragen von außerhalb des Unternehmens wirkungsvoll zu reagieren. Veröffentlichung einer Schnittstelle, über die Dritte Open-Source-Compliance-Anfragen absetzen können.  Verifikationsmaterial:  2.1.1 Eine öffentlich sichtbare Bekanntgabe einer Schnittstelle, über welche Dritte eine Open-Source-Compliance-Anfrage stellen können (z. B. durch Veröffentlichen einer Kontakt-E-Mail-Adresse oder Aufnahme in das Open Compliance-Verzeichnis der Linux Foundation).  2.1.2 Ein intern dokumentiertes Verfahren für die Bearbeitung von Open-Source-Lizenz-Compliance-Anfragen von Dritten.  Begründung:  Es soll sichergestellt werden, dass Dritte eine angemessene Möglichkeit besitzen, sich mit dem Unternehmen in Bezug auf Open-Source-Compliance-Anfragen in Verbindung zu setzen – sowie dass das Unternehmen darauf vorbereitet ist, wirkungsvoll auf dieselben zu reagieren.  2.2 Effektive Ausstattung  Identifikation der Programm-Aufgabe(n) und Ausstattung derselben mit den notwendigen Ressourcen:   * Zuweisen der Verantwortlichkeiten für die erfolgreiche Bearbeitung von Programm-Aufgaben. * Open-Source-Compliance-Aufgaben verfügen über ausreichende Ressourcen: * für die Ausführung der Aufgaben wurde ausreichend Zeit zur Verfügung gestellt; und * es wurde ein angemessenes finanzielles Budget zugewiesen. * Es existiert ein Prozess für die Entwicklung und Pflege der Richtlinie sowie für hierbei unterstützende Aufgaben; * Juristische Expertise in Bezug auf Open-Source-Compliance ist vorhanden und für diejenigen Personen verfügbar, welche hierzu eventuell Unterstützung benötigen; und * es existiert ein Prozess für die Lösung von Open-Source-Lizenz-Compliance-Problemen.   Verifikationsmaterial:  2.2.1 Ein Dokument mit den Personennamen, Gruppenzugehörigkeiten oder Funktionen, denen Programm-Rolle(n) zugeordnet sind.  2.2.2 Die identifizierten Rollen im Programm sind mit ausreichenden personellen und finanziellen Ressourcen ausgestattet  2.2.3 Benennung der juristischen Expertise, die sowohl intern als auch extern zur Adressierung von Open-Source-Compliance-Themen zur Verfügung steht.  2.2.4 Ein dokumentiertes Verfahren, das interne Verantwortlichkeiten für die Open-Source-Compliance zuweist.  2.2.5 Ein dokumentiertes Verfahren zur Prüfung und Behebung von Fällen der Nichterfüllung von Open-Source-Compliance-Anforderungen.  Begründung:  Es soll sichergestellt sein, dass i) Open-Source-Compliance-Verantwortlichkeiten tatsächlich unterstützt und mit ausreichenden Ressourcen ausgestattet sind und ii) Richtlinien und unterstützende Prozesse regelmäßig aktualisiert werden, um Änderungen in den Best Practices für Open Source-Compliance zu berücksichtigen. |

|  |  |
| --- | --- |
| 3.0 Open Source Content Review and Approval | 3.0: Überprüfung und Genehmigung von Open-Source-Inhalten |
| 3.1 Bill of Materials  A process exists for creating and managing a bill of materials that includes each Open Source component (and its Identified Licenses) from which the Supplied Software is comprised.  Verification Material(s):  3.1.1 A documented procedure for identifying, tracking, reviewing, approving, and archiving information about the collection of Open Source components from which the Supplied Software is comprised.  3.1.2 Open Source component records for the Supplied Software that demonstrates the documented procedure was properly followed.  Rationale:  To ensure a process exists for creating and managing an Open Source component bill of materials used to construct the Supplied Software. A bill of materials is needed to support the systematic review and approval of each component’s license terms to understand the obligations and restrictions as it applies to the distribution of the Supplied Software.  3.2 License Compliance  The Program must be capable of managing common Open Source license use cases encountered by Software Staff for Supplied Software, which may include the following use cases (note that the list is neither exhaustive, nor may all of the use cases apply):   * distributed in binary form; * distributed in source form; * integrated with other Open Source such that it may trigger copyleft obligations; * contains modified Open Source; * contains Open Source or other software under an incompatible license interacting with other components within the Supplied Software; and/or * contains Open Source with attribution requirements.   Verification Material(s):  3.2.1 A documented procedure for handling the common Open Source license use cases for the Open Source components of the Supplied Software.  Rationale:  To ensure the program is sufficiently robust to handle an organization’s common Open Source license use cases. That a procedure exists to support this activity and that the procedure is followed. | 3.1 Komponentenstückliste /  Bill of Materials  Es existiert ein Prozess zum Erstellen und Verwalten einer Bill of Materials, die jede Open-Source-Komponente (und ihre Identifizierten Lizenzen) enthält, aus der sich die Zugelieferte Software zusammensetzt.  Verifikationsmaterial:  3.1.1 Ein dokumentiertes Verfahren zur Identifizierung, Nachverfolgung, Prüfung, Freigabe und Archivierung von Informationen über die Gesamtheit der Open-Source-Komponenten, aus denen eine Version Zugelieferter Software besteht.  3.1.2 Eine Aufzeichnung der Open-Source-Komponenten von Zugelieferter Software, welche nachweist, dass das dokumentierte Verfahren ordnungsgemäß befolgt wurde.  Begründung:  Es soll sichergestellt werden, dass ein Prozess zum Erstellen und Verwalten einer Bill of Materials der Open-Source-Komponenten existiert, aus welchen die Zugelieferte Software besteht. Die Bill of Materials ist erforderlich, um systematisch die Lizenzbedingungen jeder Komponente zu überprüfen und freizugeben, um die Lizenzpflichten und -bedingungen im Hinblick auf die Verbreitung der Zugelieferten Software zu ermitteln.  3.2 Lizenz-Compliance  Das Programm muss es ermöglichen, die üblichen Anwendungsfälle von Open-Source-Lizenzen abzudecken, mit denen Software-Mitarbeiter im Kontext Zugelieferter Software konfrontiert sind. Zu den üblichen Fällen zählen dabei insbesondere (beachten Sie allerdings, dass die Liste weder abschließend ist, noch alle Anwendungsfälle Anwendung finden müssen):   * Verbreitung in Binärform; * Verbreitung in Sourcecode-Form; * Integration mit anderer Open-Source-Software, so dass die Voraussetzungen des Copyleft vorliegen können; * Enthält bearbeitete Open-Source-Software; * Enthält Open-Source-Software oder andere Software unter einer inkompatiblen Lizenz, die mit anderen Komponenten innerhalb der Zugelieferten Software interagiert; und / oder * Enthält Open-Source-Software mit Verpflichtungen hinsichtlich einer Nennung der Urheberschaft.   Verifikationsmaterial:  3.2.1 Ein dokumentiertes Verfahren, welches es ermöglicht, die üblichen Anwendungsfälle von Open-Source-Lizenzen für die Open-Source-Komponenten von Zugelieferter Software abzudecken.  Begründung:  Es soll sichergestellt werden, dass das Programm ausreichend robust ist, um die üblichen Anwendungsfälle von Open-Source-Lizenzen eines Unternehmens zu behandeln. Es muss gewährleistet sein, dass ein Verfahren zur Unterstützung dieser Tätigkeit besteht und dass das Verfahren befolgt wird. |

|  |  |
| --- | --- |
| 4.0 Compliance Artifact Creation and Delivery | Ziel 4: Erzeugung und Bereitstellung von Compliance-Artefakten |
| 4.1 Compliance Artifacts  A process exists for creating the set of Compliance Artifacts for the Supplied Software.  Verification Material(s):  4.1.1 A documented procedure that documents the process under which the Compliance Artifacts are prepared and distributed with the Supplied Software as required by the Identified Licenses.  4.1.2 A documented procedure for archiving copies of the Compliance Artifacts of the Supplied Software - where the archive is planned to exist for a reasonable period of time[[1]](#footnote-1) since the last offer of the Supplied Software; or as required by the Identified Licenses (whichever is longer). Records exist that demonstrate the procedure has been properly followed.  Rationale:  To ensure reasonable commercial efforts have been instituted in the preparation of the Compliance Artifacts that accompanies the Supplied Software, as required by the Identified Licenses. | 4.1 Compliance-Artefakte  Es existiert ein Prozess, um für die Zugelieferte Software die Compliance-Artefakte zusammenzustellen.  Verifikationsmaterial:  4.1.1 Ein dokumentiertes Verfahren, welches sicherstellt, dass die Compliance-Artefakte entsprechend der Anforderungen der Identifizierten Lizenzen zusammengestellt und zusammen mit der Zugelieferten Software weitergegeben werden.  4.1.2 Ein dokumentiertes Verfahren, um Kopien der Compliance-Artefakte der Zugelieferten Software zu archivieren – wobei geplant sein muss, dass das Archiv einen ausreichenden Zeitraum[[2]](#footnote-2) über das letzte Angebotsdatum einer Zugelieferten Software hinaus aufrechterhalten wird bzw. mindestens so lange, wie es die Identifizierten Lizenzen verlangen (je nachdem, welcher Zeitraum länger ist). Es existieren Aufzeichnungen als Beleg, dass das Verfahren ordnungsgemäß befolgt wird.  Begründung:  Es soll sichergestellt werden, dass angemessene Anstrengungen unternommen werden, um die der Zugelieferten Software beizufügenden Compliance-Artefakte derart zu erstellen, wie durch die Identifizierten Lizenzen erfordert. |

|  |  |
| --- | --- |
| 5.0 Understanding Open Source Community Engagement | Ziel 5: Verstehen des Engagements gegenüber der Open Source Community |
| 5.1 Contributions  If an organization permits contributions to Open Source projects then   * A written policy exists that governs contributions to Open Source projects; * the policy must be internally communicated; and * a process exists that implements the policy   Verification Material(s):  If an organization permits contributions to Open Source projects then the following must exist:  5.1.1 a documented Open Source contribution policy;  5.1.2 a documented procedure that governs Open Source contributions; and  5.1.3 a documented procedure that makes all Software Staff aware of the existence of the Open Source contribution policy (e.g., via training, internal wiki, or other practical communication method).  Rationale:  When an organization permits Open Source contributions, we want to ensure the organization has given reasonable consideration to developing and implementing a contribution policy. The Open Source contribution policy can be made a part of the overall Open Source policy or be its own separate policy. | 5.1 Beiträge  Wenn ein Unternehmen Beiträge zu Open-Source-Projekten erlaubt,   * muss eine schriftliche Richtlinie zur Regelung der Beiträge zu Open-Source-Projekten exisiteren; * muss diese Richtlinie intern kommuniziert werden * muss ein Prozess existieren, der diese Richtlinie umsetzt.   Verifikationsmaterial:  Wenn ein Unternehmen Beiträge zu Open-Source-Projekten erlaubt, muss Folgendes existieren:  5.1.1 Eine dokumentierte Richtlinie für Beiträge zu Open Source;  5.1.2 ein dokumentiertes Verfahren, welches Beiträge zu Open Source regelt;  5.1.3 ein dokumentiertes Verfahren, welches alle Software-Mitarbeiter auf die Existenz der Richtlinie für Beiträge zu Open Source aufmerksam macht (z. B. über Schulung, internes Wiki oder eine andere gängige Kommunikationsmethode).  Begründung:  Wenn ein Unternehmen Beiträge zu Open-Source-Projekten erlaubt, soll sichergestellt werden, dass das Unternehmen der Entwicklung und Umsetzung einer Richtlinie für Beiträge ausreichende Beachtung geschenkt hat. Die Richtlinie für Beiträge zu Open Source kann Teil einer übergreifenden Open-Source-Richtlinie oder eine eigene separate Richtlinie sein. |

|  |  |
| --- | --- |
| 6.0 Adherence to the Specification Requirements | 6.0: Erfüllung der OpenChain-Anforderungen |
| 6.1 Conformance  In order for a Program to be deemed OpenChain Conformant, the organization must affirm that the program satisfies the requirements presented in this specification.  Verification Material(s):  6.1.1 A document affirming the Program specified in requirement 1.4 satisfies all the requirements of this specification.  Rationale:  To ensure that if an organization declares that it has a program that is OpenChain Conforming, that such program has met all the requirements of this specification. The mere meeting of a subset of these requirements would not be considered sufficient.  6.2 Duration  A Program that is OpenChain Conformant with this version of the specification will last 18 months from the date conformance validation was obtained. The conformance validation registration procedure can be found on the OpenChain project’s website.  Verification Material(s):  6.2.1 A document affirming the Program meets all the requirements of this version of the specification (version 2.0), within the past 18 months of obtaining conformance validation.  Rationale:  It is important for the organization to remain current with the specification if that organization wants to assert program conformance overtime. This requirement ensures that the program’s supporting processes and controls do not erode if an organization continues to assert program conformance overtime. | 6.1 Konformität  Damit einem Unternehmen ein OpenChain-konformes Programm bescheinigt werden kann, muss dieses bestätigen, dass sein Programm die in der vorliegenden OpenChain-Spezifikation beschriebenen Kriterien erfüllt.  Verifikationsmaterial:  6.1.1 Ein Dokument, welches bestätigt, dass das gemäß Anforderung 1.4 definierte Programm alle Anforderungen der vorliegenden Spezifikation erfüllt.  Begründung:  Es soll sichergestellt werden, dass ein Programm alle Anforderungen dieser Spezifikation erfüllt, wenn ein Unternehmen angibt, dass sein Programm OpenChain-konform sei. Ein Erfüllen nur einzelner Anforderungen würde hierzu als nicht ausreichend erachtet.  6.2 Gültigkeitsdauer  Die Bescheinigung eines gemäß der vorliegenden Spezifikation OpenChain-konformen Programms ist ab dem Datum, zu welchem die Konformitätsprüfung bestätigt wurde, für 18 Monate gültig. Das Verfahren zur Registrierung einer Konformitätsprüfung finden Sie auf der Website des OpenChain-Projekts.  Verifikationsmaterial:  6.2.1 Ein Dokument, welches bestätigt, dass das Programm alle Anforderungen der vorliegenden Spezifikation (Version 2.0) während der vergangenen 18 Monate seit Bestätigung der Konformitätsprüfung erfüllt hat.  Begründung:  Es ist für ein Unternehmen wichtig, auf einem aktuellen Stand bezüglich der Spezifikation zu bleiben, wenn es seine Programmkonformität auf Dauer behaupten will. Diese Anforderung stellt sicher, dass die die Konformität unterstützenden Prozesse und Kontrollen des Programms nicht abgeschwächt werden, wenn ein Unternehmen die Programmkonformität über den angegebenen Zeitraum hinaus geltend machen will. |

|  |  |
| --- | --- |
| Appendix I: Language Translations | Anhang I: Sprachübersetzungen |
| To facilitate global adoption, we welcome efforts to translate the specification into different languages. Because OpenChain functions as an open source project, translations are driven by those willing to contribute their time and expertise to perform translations under the terms of the CC-BY 4.0 license and the project’s translation policy. The details of the policy and available translations can be found on the OpenChain project specification webpage. | Um die weltweite Akzeptanz zu fördern, begrüßen wir Bemühungen, die Spezifikation in mehrere Sprachen zu übersetzen. Da auch die OpenChain Initiative als Open-Source-Projekt aufgesetzt ist, werden Übersetzungen durch diejenigen gesteuert, die bereit sind, ihre Zeit und ihr Fachwissen zu Übersetzungen unter den Bedingungen der CC-BY 4.0-Lizenz und den Übersetzungs-Richtlinien des Projekts beizutragen. Die Details der Richtlinien sowie verfügbare Übersetzungen finden Sie auf der Spezifikations-Webseite des OpenChain-Projekts. |

1. determined by domain, legal jurisdiction and/or customer contracts [↑](#footnote-ref-1)
2. Abhängig von Domäne, Gerichtsstand /Rechtsordnung? und/oder Kundenverträgen [↑](#footnote-ref-2)