La conformité en questions

Contexte

Le projet OpenChain instaure la confiance dans l'open source en rendant la conformité aux licences plus simple et plus cohérente. Il gère la spécification OpenChain afin de définir un ensemble d'exigences de base que chaque programme de conformité de qualité doit satisfaire. Le résultat est que la conformité aux licences open source devient plus prévisible, plus compréhensible et plus efficace pour les participants de la chaîne d'approvisionnement en logiciels.

Ce document contient une série de questions permettant de déterminer si une entreprise dispose d'un programme de conformité OpenChain. Si la réponse à chacune de ces questions est affirmative, alors cette entreprise satisfait à toutes les exigences de conformité à la spécification OpenChain version 2.1 (fonctionnellement identique à ISO/IEC DIS 5230:2020(e)). Si la réponse à l'une de ces questions est négative, l'entreprise peut alors clairement identifier les domaines dans lesquels un investissement supplémentaire est nécessaire pour améliorer le processus de conformité.

1. Fondamentaux du programme

Section	Numéro	Référence dans la spé cification	Texte de la question
1. Fondamentaux du programme	1.a	1.1, 1.1.1	Disposez-vous d'une politique documentée qui régit la conformité aux licences open source du logiciel fourni ?
1. Fondamentaux du programme	1.b	1.1, 1.1.2	Disposez-vous d'une procédure documentée pour communiquer l'existence de cette politique open source à tous les participants au programme
1. Fondamentaux du programme	1.c	1.2, 1.2.1	Avez-vous identifié les rôles et responsabilités qui garantissent la performance et l'efficacité programme ?
1. Fondamentaux du programme	1.d	1.2, 1.2.2	Avez-vous identifié et documenté les compétences requises pour chaque rôle ?
1. Fondamentaux du programme	1.e	1.2, 1.2.3	Avez-vous documenté les compétences évaluées pour chaque participant au programme ?
1. Fondamentaux du programme	1.f	1.3, 1.3.1	Avez-vous documenté le degré de sensibilisation des participants au programme sur les sujets suivants ?
1. Fondamentaux du programme	1.f.i	1.3	- La politique open source et où la trouver ;
1. Fondamentaux du programme	1.f.ii	1.3	- Les objectifs pertinents de l’open source ;
1. Fondamentaux du programme	1.f.iii	1.3	- Les contributions attendues pour assurer l'efficacité du programme ;
1. Fondamentaux du programme	1.f.iv	1.3	- Les conséquences du non-respect des exigences du programme.
1. Fondamentaux du programme	1.g	1.4, 1.4.1	Avez-vous un processus pour déterminer le champ d'application de votre programme ?
1. Fondamentaux du programme	1.h	1.4, 1.4.1	Avez-vous une déclaration écrite qui définit clairement le champ d'application et les limites du programme ?
1. Fondamentaux du programme	1.i	1.5, 1.5.1	Avez-vous une procédure documentée pour examiner et documenter les obligations, restrictions et les droits liés aux licences open source ?

2. Définition des tâches nécessaires et des ressources associées

Section	Numéro	Référence dans la spé cification	Texte de la question
2. Définition des tâches nécessaires et des ressources associées	2.a	2.1, 2.2.1	Avez-vous confié à une ou plusieurs personnes la responsabilité de recevoir les demandes externes relatives à la conformité open source ?
2. Définition des tâches nécessaires et des ressources associées	2.b	2.1, 2.1.1	Le contact externe pour la conformité des logiciels open source est-il identifié publiquement (par une adresse électronique ou le répertoire de conformité de la Fondation Linux, etc.) ?
2. Définition des tâches nécessaires et des ressources associées	2.c	2.1, 2.1.2	Avez-vous une procédure documentée pour recevoir et répondre aux demandes relatives à la conformité des logiciels open source ?
2. Définition des tâches nécessaires et des ressources associées	2.d	2.1, 2.2.1	Avez-vous documenté les personnes, groupes ou fonctions pour chaque rôle identifié au sein du programme ?
2. Définition des tâches nécessaires et des ressources associées	2.e	2.1, 2.2.2	Est-ce que les rôles définis pour le programme ont été suffisamment pourvus en personnel et bénéficient d'un financement adéquat ?
2. Définition des tâches nécessaires et des ressources associées	2.f	2.1, 2.2.3	Les compétences juridiques nécessaires pour répondre à la conformité interne et externe open source sont-elles identifiées ?
2. Définition des tâches nécessaires et des ressources associées	2.g	2.1, 2.2.4	Avez-vous une procédure documentée attribuant les responsabilités internes en matière de conformité à l'open source ?
2. Définition des tâches nécessaires et des ressources associées	2.h	2.1, 2.2.5	Avez-vous une procédure documentée pour traiter l'examen et la correction des cas de non-conformité ?

3 Examen et validation des contenus open source

Section	Numéro	Référence dans la spé cification	Texte de la question
3 Examen et validation des contenus open source	3.a	3.1, 3.1.1	Avez-vous une procédure documentée pour identifier, suivre et archiver les informations au sujet de l'ensemble des composants open source dans une version du logiciel fourni ?
3 Examen et validation des contenus open source	3.b	3.1, 3.1.2	Avez-vous des archives sur les composants open source du logiciel fourni qui démontrent que la procédure documentée a été correctement suivie ?
3 Examen et validation des contenus open source	3.c	3.2, 3.2.1	Avez-vous une procédure documentée qui couvre les cas d'utilisation de licences open source communes pour les composants open source dans le logiciel fourni ?
3 Examen et validation des contenus open source	3.c.i	3.2, 3.2.1	- distribué sous forme de binaire ;
3 Examen et validation des contenus open source	3.c.ii	3.2, 3.2.1	- distribué sous forme de code source ;
3 Examen et validation des contenus open source	3.c.iii	3.2, 3.2.1	- intégré à d'autres logiciels open source qui peuvent entraîner des obligations supplémentaires ;
3 Examen et validation des contenus open source	3.c.iv	3.2, 3.2.1	- contient du code open source modifié ;
3 Examen et validation des contenus open source	3.c.v	3.2, 3.2.1	- contient du code open source ou du code diffusé sous une licence incompatible qui interagit avec d'autres composants du logiciel fourni ;
3 Examen et validation des contenus open source	3.c.vi	3.2, 3.2.1	- contient du code open source avec des exigences d'attribution.

4. Création et fourniture de livrables de conformité

Section	Numéro	Référence dans la spé cification	Texte de la question
4. Création et fourniture de livrables de conformité	4.a	4.1, 4.1.1	Avez-vous une procédure documentée qui décrit le processus selon lequel les livrables de conformité sont distribués avec le logiciel fourni comme requis par les licences identifiées ?
4. Création et fourniture de livrables de conformité	4.b	4.1, 4.1.2	Avez-vous une procédure documentée pour archiver des copies des livrables de conformité pour le logiciel fourni ?
4. Création et fourniture de livrables de conformité	4.c	4.1, 4.1.2	Est-ce que les livrables de conformité sont archivés aussi longtemps que le logiciel fourni est diffusé et comme requis par les licences identifiées ?

5. Comprendre les engagements de la communauté open source

Section	Numéro	Référence dans la spé cification	Texte de la question
5. Comprendre les engagements de la communauté open source	5.a	5.1, 5.1.1	Avez-vous une politique de contribution aux projets open source pour l'organisation ?
5. Comprendre les engagements de la communauté open source	5.b	5.1, 5.1.2	Avez-vous une procédure documentée régissant les contributions open source ?
5. Comprendre les engagements de la communauté open source	5.c	5.1, 5.1.3	Avez-vous une procédure documentée pour sensibiliser l'ensemble des participants au programme à la politique de contribution aux projets open source ?

6. Conformité aux exigences de la spécification

Section	Numéro	Référence dans la spé cification	Texte de la question
6. Conformité aux exigences de la spécification	6.a	6.1, 6.1.1	Avez-vous des documents qui confirment que votre programme répond à toutes les exigences de cette spécification ?
6. Conformité aux exigences de la spécification	6.b	6.2, 6.2.1	Avez-vous des documents qui confirment que la conformité de votre programme a été examinée au cours des 18 derniers mois ?