Checklisten

Ein Zitat, welches man in Bezug auf die Aspekte des Compliance-Engineerings im Hinterkopf behalten sollte, stammt von C. Northcote Parkinson:

> "*Arbeit dehnt sich in genau dem Maß aus, wie Zeit für ihre Erledigung zur Verfügung steht.*"

Bei richtiger Anwendung kann die Arbeit mit Checklisten ein sehr nützlicher Weg sein, Aufgaben im Bereich GPL-Compliance schnell, konsistent und effektiv zu organisieren. Bei falscher Anwendung jedoch können sie für konkret anstehende Arbeiten entweder zu Allgemeingültig sein – oder im Gegenzug zu überwältigenden Aufgabenlisten eines schier endlosen Reviews werden. Der 'goldene Mittelweg' ist das Ziel. Worin dieser 'goldene Mittelweg' besteht, hängt effektiv von der Größe des zu betrachtenden Unternehmens ab.

Eine kurze und einfache Checkliste ist die 'Allgemeine Compliance Checkliste'. Diese wurde aus den Präsentationsunterlagen des *OpenChain-Curriculums*[1] zusammengestellt. Diese - wiederum – basieren auf der Open Compliance *Self-Assessment Compliance Checklist*[2] der Linux Foundation. Die Checkliste empfiehlt sich für kleine Unternehmen – oder dafür, in großen Unternehmen das Generalthema zu umreißen.

Um bestimmte Compliance-Ziele zu adressieren, kann die Auswahl einer spezifischeren Checkliste sinnvoll sein. Zum Beispiel ist die Behandlung des Bereichs "vollständiger und zugehöriger Quellcode" wohl der erste und nützlichste Anwendungsbereich für eine spezifische Prüfliste. Eine Möglichkeit, diese aufzustellen, wäre, eine erschöpfende Liste aller möglichen und notwendigen Schritte anzufertigen. Ein anderer Weg bestünde darin, den "Kern" des Problems abzudecken und Details bei Bedarf durch gesondert geschultes Personal oder über Unter-Checklisten behandeln zu lassen. Als Beispiel für Letzteres siehe "Checkliste für den Rebuild von Produkt X".

Es gibt viele Möglichkeiten für umfassendere Checklisten. Ein guter Anfang ist die *Self-Assessment Compliance Checklist*. Diese durchläuft den gesamten Prozess und ist eine Checkliste, wie sie für eine größere Organisation erforderlich sein kann. Diese Checkliste ist wie das oben genannte Material kostenlos und frei verfügbar, so dass Sie herausfinden können, was Ihren Anforderungen am besten entspricht.

---

[1] https://www.openchainproject.org/curriculum

[2] https://www.linuxfoundation.org/projects/opencompliance/self-assessment-compliance-checklist

Allgemeine Compliance Checkliste

Schritt #1: Laufende Compliance-Aufgaben

- ❏ Jegliche FOSS wird im Beschaffungs- / Entwicklungszyklus frühzeitig erkannt.
- ❏ Alle genutzten FOSS-Pakete werden reviewt und freigegeben.
- ❏ Die zur Erfüllung der FOSS-Verpflichtungen nötigen Informationen werden verifiziert.
- ❏ Jegliche das Unternehmen verlassende Kontributionen zu FOSS-Projekten werden reviewt und freigegeben.

Schritt #2: unterstützende Voraussetzungen

- ❏ Eine angemessene Personalausstattung ist sichergestellt und klare Verantwortungsbereiche wurden festgelegt.
- ❏ Bestehende Geschäftsprozesse wurden in Hinsicht auf eine Unterstützung des FOSS-Compliance-Programms angepasst.
- ❏ Schulungen zur Unternehmens-FOSS-Policy sind für jeden Mitarbeiter verfügbar.
- ❏ Der Fortschritt aller Compliance-Aktivitäten wird überwacht.

Checkliste für den Rebuild von Produkt X

Diese Checkliste kann Teil des Review-Prozesses sein, um sicherzustellen, dass "vollständiger und korrespondierender" Quellcode verfügbar ist, wenn Produkte mit GPL-Code distribuiert werden.

Schritt #1

- ❏ Wird eine vollständige Beschreibung der Build-Umgebung bereitgestellt? (Diese sollte Paketversionen sowie ähnliche Information enthalten, die für die Compliance-Sicherstellung kritisch ist)

Schritt #2

- ❏ Wird eine Liste der Rebuild-Schritte bereitgestellt?

Schritt #3

- ❏ Konnte ein Rebuild auf einem “sauberen” System erfolgreich abgeschlossen werden?

Schritt #4

- ❏ Wurden die Rebuild-Ergebnisse verifiziert?

Schritt #5

- ❏ Wurden irgendwelche Unklarheiten an das Open-Source-Support-Team eskaliert?