Checklists

A quotation worth bearing in mind with regards all aspects of compliance engineering comes from C. Northcote Parkinson:

"*Work expands so as to fill the time available for its completion.*"

When used properly checklists can be a useful way to manage your GPL compliance tasks in a quick, consistent and effective manner. When used incorrectly they can be too general to cover the work at hand or become overwhelming task lists requiring endless review. A happy medium is the goal. What constitutes a happy medium really depends on your organizational size.

See the 'General Compliance Checklist' for a short and simple checklist. This is from the *OpenChain Curriculum slides*.[1] It is based - in turn - on the Linux Foundation Open Compliance Program *Self-Assessment Compliance Checklist*.[2] It may be suitable for a small organization or for framing the general issue for a large organization.

You might elect to have more specific checklists to address specific compliance goals. For example, the concept of addressing the "complete and corresponding" source code for distribution is arguably the first and most useful area to have a specific checklist. One way of approaching this would be to create an exhaustive list of all the steps possible and necessary. Another way would be to cover the "core" of the issue and leave details to trained personnel or sub-checklists as needed. See 'Checklist For Rebuilding Product X' for an example of the latter.

Plenty of options exist for more comprehensive checklists. A great place to start is the Open Compliance Program *Self-Assessment Compliance Checklist*. This is a more detailed list running through the whole process and may be required for a larger organization. This checklist, like the material above, is free of charge and freely available so you can explore what is best to meet your requirements.

---

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

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

General Compliance Checklist

Step #1: Ongoing Compliance Tasks

- ❏ Discover all FOSS early in the procurement/development cycle.
- ❏ Review and Approve all FOSS packages used.
- ❏ Verify the information necessary to satisfy FOSS obligations.
- ❏ Review and approve any outbound contributions to FOSS projects.

Step #2: Support Requirements

- ❏ Ensure adequate compliance staffing and designate clear lines of responsibility.
- ❏ Adapt existing business processes to support the FOSS compliance program.
- ❏ Have training on the organization’s FOSS policy available to everyone.
- ❏ Track progress of all compliance activities.

Checklist For Rebuilding Product X

This checklist can be part of the review process for ensuring “complete and corresponding” source code is available when distributing products containing GPL code.

Step #1

- ❏ Is a complete description of the build environment provided?
  (This should include package versions and any similar information critical to ensuring compliance.)

Step #2

- ❏ Is a list of rebuild steps provided?

Step #3

- ❏ Has a rebuild been successfully completed on a clean machine?

Step #4

- ❏ Have the rebuild results been verified?

Step #5

- ❏ Have any uncertainties been escalated to the Open Source support team?