OPEN SOURCE COMPLIANCE

Recommended Practices For Compliance Professionals

- Compliance is verified on a product-by-product basis: If an open source component is approved for use in one product, it does not necessarily mean it is pre-approved for use in other products.
- Scan all source code, early and often. It allows you to discover compliance problems as they occur, provide solutions within acceptable delays, and perform incremental compliance very efficiently.
- Inspect and resolve each file or snippet flagged by the scanning tool.
- When in doubt with the scan results discuss with engineering.
- Identify all the components and snippets included in the product, their origin and licenses.
- Scan newer used versions of previously approved packages.
- If the scanning tool identifies GPL-licensed source code (for instance) integrated in a proprietary component, report to Engineering and request correction. Re-scan the code after Engineering has resolved the issue to get a solid confirmation that GPL code has been replaced.
- In preparation of legal review, provide Legal with all licensing information discovered in the component. For open source components, that includes COPYING, README, or LICENSE files.
- If there are conflicts or compliance is not possible:
    a. Remove / Replace: Can you live without this code? Is there an alternative project with same function under a different license?
    b. Re-engineer: Can you create a work around?
    c. Version tracking: Is there a newer (or older) version of this code under a different license?
    d. Re-license: Can you contact the author(s) and ask for a different license?
- Be clear in the language of the written offer and the open source notices; be inclusive to all open source included in the product.

Ibrahim Haddad, Ph.D.

Twitter: @IbrahimAtLinux