Open
Source
Automation
Development
Lab eG

OSADL License Compliance Audit (OSADL LCA)

1. Goals

Risk management for any company includes the maintenance of legal and contractual obligations. The observance of these obligations as well as any internal guidelines is covered by the term "compliance." The maintenance of legal requirements and internal guidelines as dictated by the compliance management system is organized and audited using recognized standards such as IDW PS 980.

Experience shows that maintaining Open Source licenses under existing compliance systems has not lead to satisfactory results. This may be due to the particular complexity of the legal guidelines and certain incompatibilities between technology and the law. OSADL has therefore assumed the responsibility of developing its own auditing process to ensure that the obligations arising from Open Source licenses are maintained. Initially, this auditing system will be offered for products in which the Linux kernel and associated access libraries are used.

OSADL thereby aims to help its members use associated products in compliance with the law. Since violating the conditions of Open Source licenses such as the GNU General Public License (GPL) can lead to the copyright infringement, licensors can forbid the further distribution of non-compliant products. In addition, reputations can be damaged, and related suits can cost a considerable amount of money.

By using a special auditing process, the OSADL License Compliance Audit (OSADL LCA), companies who use Linux within their embedded systems can determine whether the necessary measures have been taken to satisfy the obligations associated with Open Source licenses. This ensures that Open Source software is used in a compliant manner.

2. Product-related approach

An OSADL LCA always relates to specific products even when there are additional audits of internal company processes to determine their compliance with the conditions of Open Source licenses. This is because the OSADL audit specifically determines whether there is actual legal and technical compliance with the GPL as opposed to a general audit. This makes OSADL a trailblazer in the field of license compliance.

The technical analysis examines chiefly whether the available source code satisfies the conditions of the GPL or LGPL. This adds an important and frequently underestimated review to the auditing of references. In addition, the used source code is checked for deviations in comparison to a specific set of standard Linux kernels. This allows the identification of relevant changes to modified versions of software to determine their compliance. It is, however, assumed that a stable version of the Linux kernel released by kernel maintainers and available from the kernel repository on the Internet at kernel.org has already had undergone a sufficient license audit. This assumption must either be accepted or investigated by every company within the context of their risk management system.

3. Scope of the audit

The OSADL LCA determines whether the Open Source license conditions have been observed for the Linux kernel used in an embedded system and the C Library used in the kernel (such as glibc). However, not every single application program is checked in the user space and the bootloaders. This provides a consistent auditing standard with clearly defined criteria. A wide range of approaches are used for the user space which may not contain any open source software, or numerous different software components with different license conditions may be used. Consequently, the review needs to be tailored to the specific instance which lies outside the scope of the OSADL LCA. Nevertheless, the reviews of internal processes executed within the audit can provide indications of problems.

The OSADL LCA primarily focuses on compliance with license conditions relating to authorizations associated with copyrights. The potential violation of third-party patents is not reviewed. Such patents may not be used without the approval of the patent owner. Every user of the open source program is responsible for identifying the related patents and determining whether appropriate coverage is provided by licenses for the user's own patents.

4. Relevant Open Source licenses

The Linux kernel is licensed under version 2 of the GPL. The GNU C Library (glibc) is licensed under version 2.1 of the GNU Lesser General Public License. Individual files or components can be licensed under so-called non-copyleft licenses such as the BSD license that, however, do not contain any obligations that transcend the GPL and LGPL. The OSADL LCA focuses on auditing the license conditions of the GPL and LGPL.

The GPL has already been involved in several legal challenges in Germany (such as cases heard by Munich District Court I: Welte vs. Sitecom, Welte vs. D-Link Deutschland GmbH, WLAN Router, Welte vs. Skype Technologies S.A., AVM vs. Cybits). The suits involved compliance with license conditions of the GPL. The related companies were barred from marketing their products if the conditions of the license were not observed. This illustrates the importance of compliance as well as the enforceability of Open Source licenses before the court. Related suits have also been filed in the United States, although they have been settled out of court so far (see http://www.softwarefreedom.org/news/2007/sep/20/busybox/).

5. Details of the audit

The license obligations and prohibitions are listed below which underlie the reference standard used in the OSADL LCA.

a) Provision of the license text

Clauses 1 and 3 GPL:
„You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that ...; and give any other recipients of the Program a copy of this License along with the Program.“
„You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above ...“

Clauses 1 and 4 LGPL:
„You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that ...; and distribute a copy of this License along with the Library.“
„You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above...“

- Hardcopy – electronic form – online
- Supplement to the kernel license
- Language version

b) Notation of copyright

Clauses 1 and 3 GPL:
„You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty.“
„You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above ...“

Clauses 1 and 4 LGPL:
„You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty;“
„You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above...“

- Differentiation based on distribution with or without source code
- Scope and practicality
- Automatic extraction of notations of copyright

c) Disclaimer

Clauses 1 and 3 GPL:
„You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty“
„You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above ...“

Clauses 1 and 4 LGPL:

„You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty;“
„You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above...“

- Differentiation according to "written offer" and supply of source code
- Review of formulation of the text
- Relationship to warrantees for the entire embedded system

d) Provision of "Complete Corresponding Machine-readable Source Code"

Clause 3 GPL:

> *„**a)** Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,*
> ***b)** Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,*

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.“

Clauses 4 and 6 LGPL:

> *„... accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.“*
> *„c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.“*

- Written offer or direct supply
- Determine correspondence by reconstructing the compilation process on-site
- Check the information for rebuilding the toolchain – scripts to control compilation and installation
- Check the installation of modified kernel versions
- Check whether systems provide the source code of previous versions
- Check the provision of source code when firmware is used online

e) Compliance with license conditions for modified software

Clause 2 GPL:

> ***„a)** You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.*

> ***b)*** *You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.*
> ***c)*** *If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)"*

Clause 5 LGPL:

> **a)** The modified work must itself be a software library.
>
> **b)** You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.
> **c)** You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.
> **d)** If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.
>
> *(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)*

- Check whether there are deviations from defined standard Linux kernels using corresponding software tools
- Modified files: Check licensing under the GPL or a compatible license
- Modified files: Determine whether the release was provided by an authorized representative and the necessary copyrights were obtained
- Modified files: Check the reference to the change and date
- Requirements of the "Signed-off-by" for code provided for mainline kernel

f) Inspect accompanying documentation

Clause 6 GPL:
„You may not impose any further restrictions on the recipients' exercise of the rights granted herein."

Clause 10 LGPL:
„You may not impose any further restrictions on the recipients' exercise of the rights granted herein."

- Inspect the manual
- Review the license text, contractual conditions, and EULAs for the product

g) Relinking of the C library

Clause 6 LGPL:

> „***a)*** *Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)*
> ***b)*** *Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.*
> ***c)*** *Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.*
> ***d)*** *If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.*
> ***e)*** *Verify that the user has already received a copy of these materials or that you have already sent this user a copy.*

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable. "

h) Permission of modification

Clause 6 LGPL:
„...provided that the terms permit modification of the work for the customer's own use..."

i) Permission of reverse engineering

Clause 6 LGPL:
„...provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications."

6. Audit report

The license obligations and prohibitions are listed below which underlie the reference standard used in the OSADL LCA.

After the audit is performed, the client will be given a report that summarizes the results of the individual steps, lists problems, and notes the degree of compliance with the license conditions for the audited product. The audit does not represent a confirmation of conformance; it rather is a list of results indicating the degree of compliance with the individual conditions of the Open Source licenses. If all of the necessary conditions have been satisfied as far as can be discerned, the client is issued a certificate along with the report.

7. Auditors

The audits are performed jointly by **JBB Attorneys** and **Tjaldur Software Governance Solutions** for OSADL.

JBB Attorneys in Berlin are specializing in trademarks and competition law, copyright and media law as well as IT and data protection law. An important area of focus are legal aspects of Free and Open Source Software. With respect to this topic, JBB is advising developers and enterprises and has considerable forensic activities.

Tjaldur Software Governance Solutions is a company from the Netherlands specialized in software governance and license compliance engineering. Tjaldur has specific expertise in GNU GPL and LGPL license compliance. Its flagship product is the Binary Analysis Tool to scan object code and search for possible copyright violations.