

FOSS CON KOREA 2017

공개SW 거버넌스 구축 사례

2017. 11. 20

Software Center OSC



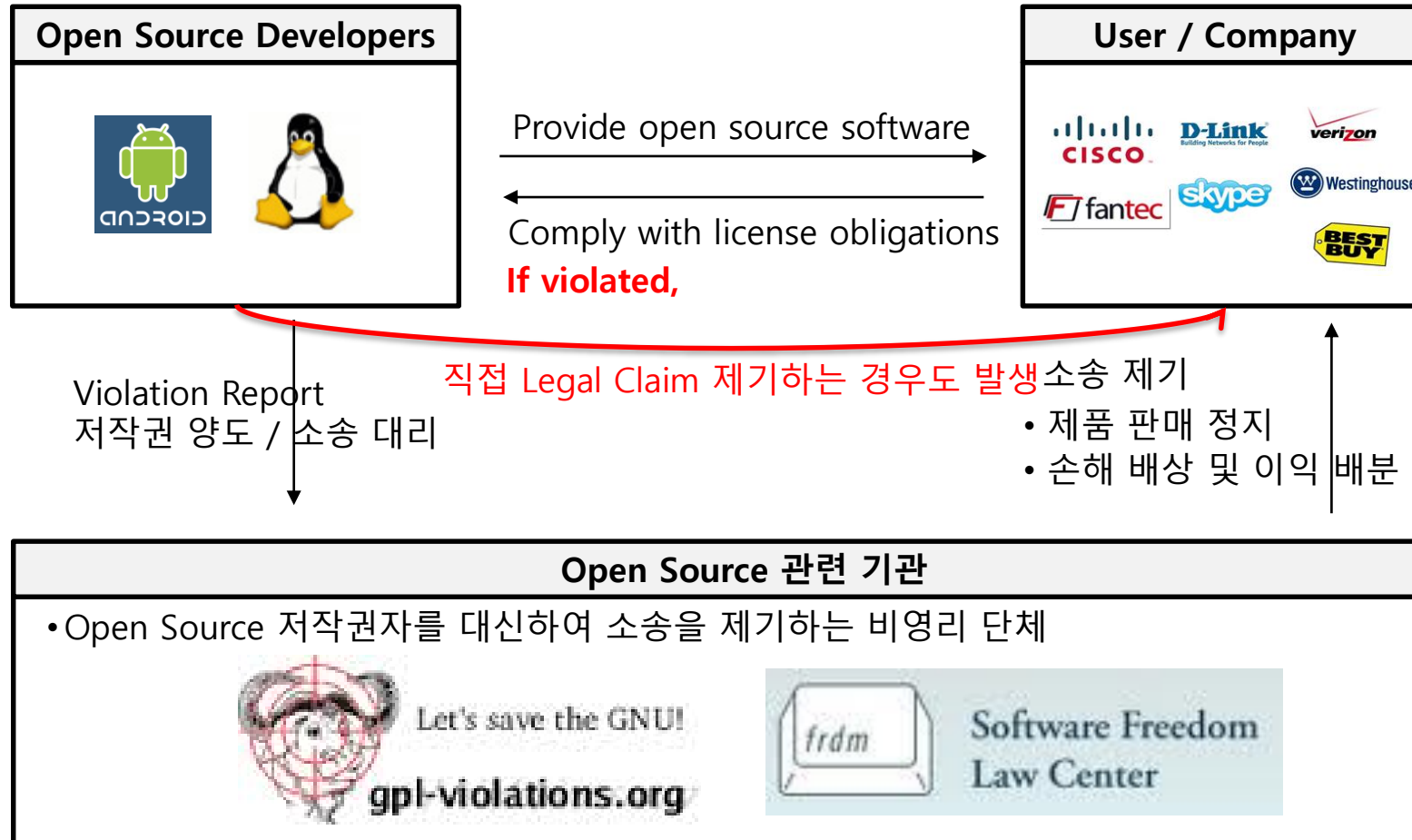
Contents

- ❑ Open Source Risk
- ❑ Open Source Compliance Process
- ❑ Compliance Activities
- ❑ Open Source Community Tool 활용
 - SPDX
 - FOSSology
 - OpenChain

Open Source Risk

Open Source Risk

- Open Source를 사용하면서, License를 위반하는 기업은 소송을 제기 당할 수 있음

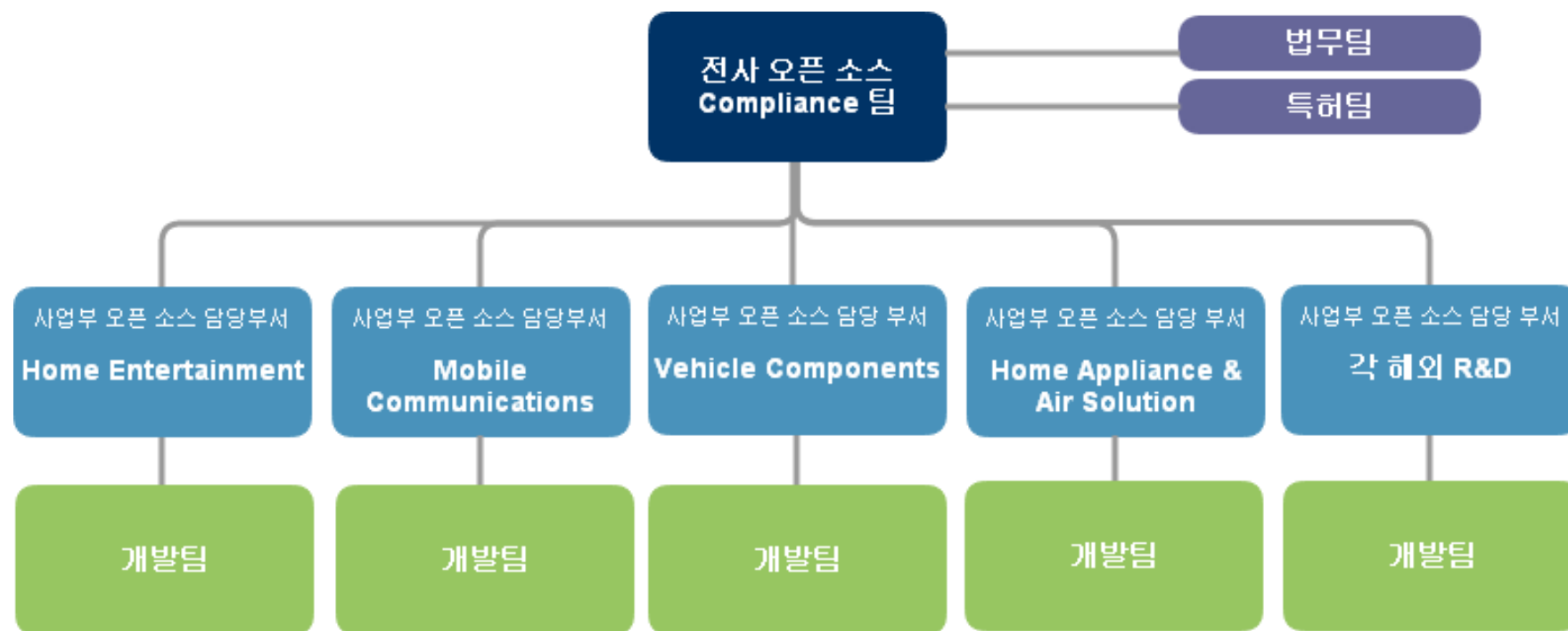


No Compliance is Expensive

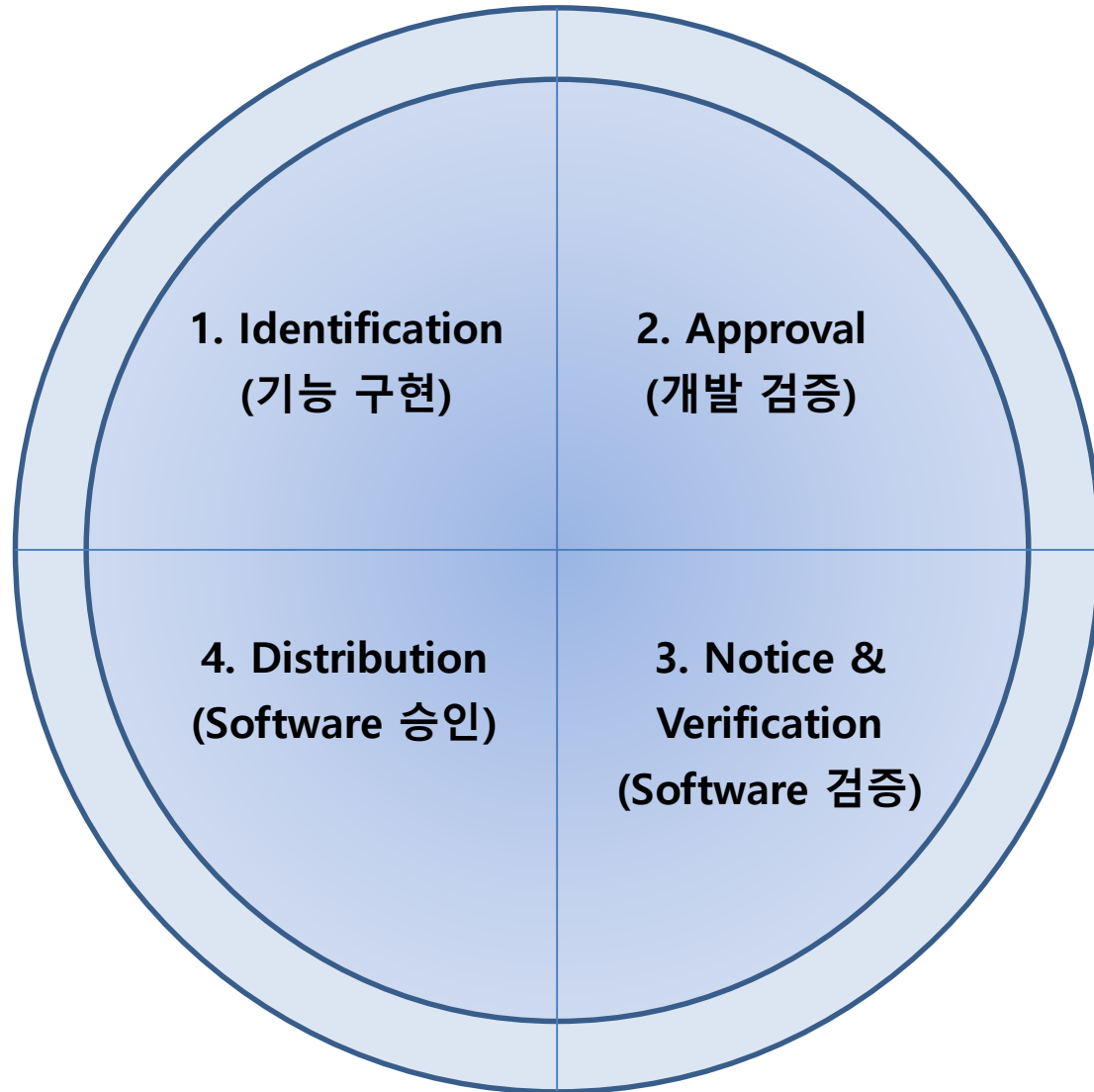
- 위반이 발생할 경우, 이를 해결하기 위해서는 상당한 비용이 발생함
 - Compliance 위반 문의 접수 시, 기업은 이를 조사하고 분석하기 위한 비용 발생
 - 고소인과의 합의를 위한 비용
 - 변호사 비용
 - Brand와 명성, 신용에 대한 타격
 - 사회적인 이슈
 - 언론의 비판
 - 고객사, Supplier, 유력 Open Source Community / 기관 등과의 관계 악화

Open Source Compliance Process

Open Source Compliance 조직



LG전자 Open Source Compliance 단계



1단계 : Identification (기능 구현) : License Identification

- OSC System (<http://osc.lge.com>) 통한 Open Source License 확인

OSS Name		Copyright Text		Search
License Name		Description		
WebSite		Vulnerability	CVE -	

Excel download

ID	OSS Type ?	OSS Name	Version	License Name	License Ty	Obligation ?	Download Location	Homepag	Description	Vulnerability
981		perl-podlators	2.5.1	Artistic-1.0-Perl	Permissive		http://search.cpan.org/~L...			
3818		perl-DBD-MySQL	4.023	Artistic-1.0-Perl	Permissive		http://s...			
2852		perl-XML-Parser		GPL-2.0 OR Artistic-1.0	Copyleft		http://s...			
583		perl-Pod-Escapes	1.04	Artistic-1.0-Perl	Permissive		http://s...			
4896		android-SimpleCursorLoa		Apache-2.0	Permissive		http://s...			
2363		Apache ServiceMix :: Fea	4.5.3	Apache-2.0	Permissive		http://n...			
6615		Javax.servlet API V.2.5	3.1.1	CDDL-1.0 AND GPL-2.0-with-d	Copyleft		https://			
+ 196		Isscsi	0.27	GPL-2.0	Copyleft		http://s...			
+ 6453		sdparm	1.08	BSD-3-Clause	Permissive		http://s...			
2368		Silverlight Toolkit		MS-PL	Permissive		http://s...			
+ 2980		SimpleXML	2.7.1	Apache-2.0	Permissive		http://s...			
+ 6340		tiff	4.0.7	libtiff	Permissive		http://d...			
+ 5940		icu	57.1	ICU	Permissive		http://s...			
2264		dragdealer		MIT	Permissive		https://			
+ 2384		smartmontools	6.2	GPL-2.0	Copyleft		https://			

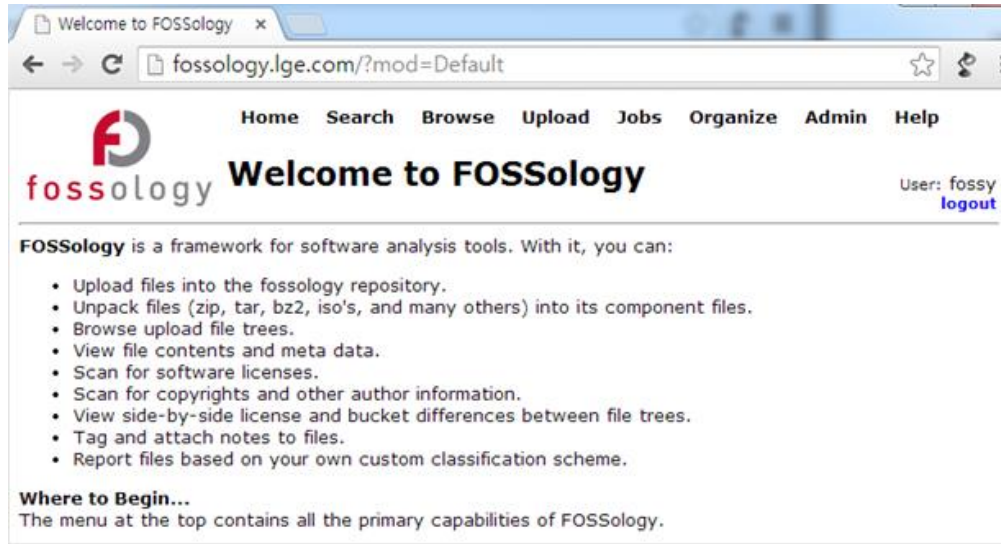
Page 50 of 234

OSS Name	BusyBox
Nick Name	tinylogin
OSS Version	1.4
License	Single License
Show license text	GNU General Public License v2.0 only
Copyright	Copyright (c) 1999-2008 Erik Andersen
License Type	Copyleft
Obligation	
Download Location	https://busybox.net/downloads/
Home Page	https://www.busybox.net/
Summary Description	

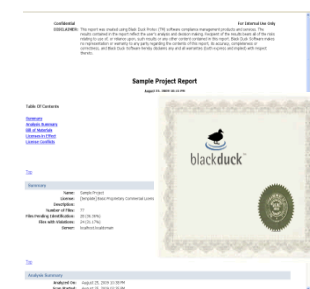
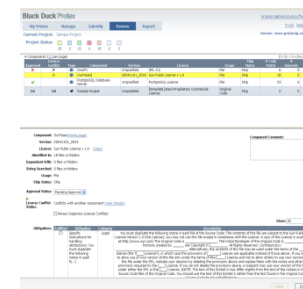
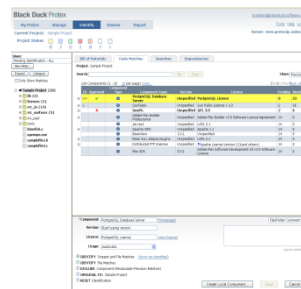
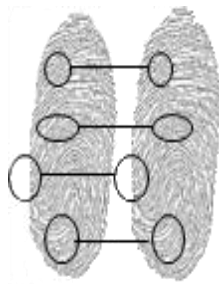
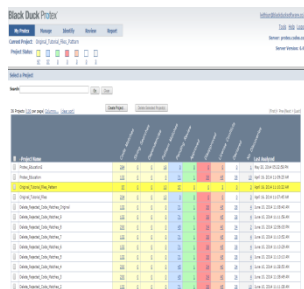
2단계 : Approval (개발 검증) - Source Code 분석

❑ Source Code 분석 : Source Code level에서 Open Source Software 사용 여부 및 License 확인

■ FOSSology



■ Black Duck Protex



2단계 : Approval (개발 검증) – OSS 보고서

□ 확인한 사항을 기반으로 OSS 보고서 작성

ID	3rd Party	Binary Name	OSS Name	OSS Version	License	Download Location	Homepage	Copyright Text
-	[Software 공급회사 이름]	[Binary Name]	[사용한 Open Source]	[Open Source]	[Open Source의 License]	[Open Source를 Download한 위치]	[Open Source의 Homepage]	[OSS의 Copyright 정보. 예: Copyright (c) 1999-2008 Erik Andersen]
1	Creative Company	creative.so	busybox	0.60.3	GPL-2.0	https://busybox.net/download	https://www.busybox.net	Copyright (c) 1999-2008 Erik Andersen
2								
3								

ID	Source Name or Path	OSS Name	OSS Version	License	Download Location	Homepage	Copyright Text
-	[Source File 혹은 Path]	[사용한 Open Source]	[Open Source]	[Open Source의 License]	[Open Source를 Download한 위치]	[Open Source의 Homepage]	[OSS의 Copyright 정보. 예: Copyright (c) 1999-2008 Erik Andersen]
1	/src/tools/busybox/	busybox	1.4	GPL-2.0	https://busybox.net/download	https://www.busybox.net	Copyright (c) 1999-2008 Erik Andersen
2	/src/framework/curl/	curl	7.50.3	curl	https://github.com/curl/curl	http://curl.haxx.se	Copyright (c) 1996 - 2015, Daniel Stenberg
3	/src/application/calendar/view.c	-		BSD-3-Clause			Copyright (c) 2016, NetBSD

ID	Binary Name	OSS Name	OSS Version	License	Download Location	Homepage	Copyright Text
-	[Binary/Library File 이름]	[사용한 Open Source]	[Open Source]	[Open Source의 License]	[Open Source를 Download한 위치]	[Open Source의 Homepage]	[OSS의 Copyright 정보. 예: Copyright (c) 1999-2008 Erik Andersen]
1	creative.so	busybox	0.60.3	GPL-2.0	https://busybox.net/download	https://www.busybox.net	Copyright (c) 1999-2008 Erik Andersen
2							
3							

3단계 : Notice & Verification (Software 검증) – OSS 고지문구

□ OSS 고지 문구 (OSS Notice)

- 사용된 Open Source 및 License를 외부에 고지하기 위한 문서 (각 License의 원문 전체를 포함)
- Source code 수령방법에 대해 안내

LGE Open Source Software Notice

OSSNotice-485_Sample_170305.html

This product from LG Electronics, Inc. ("LGE"), contains the open source software detailed below. Please refer to the indicated open source licenses (as are included following this notice) for the terms and conditions of their use.

Open Source	License	Copyright
cairo 1.10.2	LGPL-2.1	Copyright (C) 2010. Chris Wilson <chris@chris-wilson.co.uk>
Linux Kernel 3.1.10	GPL-2.0	
U-Boot v2011.06	GPL-2.0	Copyright (c) 2002-2015 by DENX Software Engineering
alsa-lib 1.0.23	LGPL-2.1	Copyright © 2002-2015 Judd Vinet and Aaron Griffin.
DirectFB 1.2.7	LGPL-2.1	Copyright (c) 2001-2008 The world wide DirectFB Open Source Community (directfb.org) Copyright (c) 2000-2004 Convergence (integrated media) GmbH Written by Denis Oliver Kropp <dok@directfb.org>, Andreas Hundt <andi@fischlustig.de>, en Neumann <neo@directfb.org>, Ville Syrjälä <syrjala@sci.fi> and laudio Ciccani <klan@users.sf.net>.

The source code for the above may be obtained free of charge from LGE at <http://opensource.lge.com>. LGE will also provide open source code to you on CD-ROM for a charge covering the cost of performing such distribution (such as the cost of media, shipping, and handling) upon email request to opensource@lge.com. This offer is valid for three (3) years from the date on which you purchased the product.

3단계 : Notice & Verification (Software 검증) –Packaging

□ 공개할 Source Code를 취합하여 하나의 파일로 압축 (Package)

이름	수정한 날짜	유형
이름		
Linux Kernel 3.1.10	2017-04-09 오후...	파일 폴더
U-Boot_V2011.06.tar.gz	2017-04-09 오후...	ALZip GZ File
2017-04-09 오후...	파일 폴더	
2017-04-09 오후...	파일	

LGE Open Source Software Notice

This product from LG Electronics, Inc. ("LGE"), contains the open source software detailed below. Please read the following notice for the terms and conditions of their use.

Open Source	License	
cairo 1.10.2	LGPL-2.1	Copyright (C) 2010. Chris Wilson
Linux Kernel 3.1.10	GPL-2.0	
U-Boot v2011.06	GPL-2.0	Copyright (c) 2002-2015 by DENX

The source code for the above may be obtained free of charge from LGE at <http://opensource.lge.com> or a charge covering the cost of performing such distribution (such as the cost of media, shipping, etc.) may be charged. This offer is valid for three (3) years from the date on which you purchased the product.

Please be informed that LG Electronics, Inc. products may contain open source software listed in the following table:

Project Name

Temp for Mailing Test (2) B I D

Created

u_wonjae.park CTO SW센터 (2017-05-17)

Packaging

☐ Approve without verification

Reject

Comment Edit

Change Path

Upload

 Drag & Drop Files

export

* Open Source List to disclose source code							
ID	Referen	OSS Name	OSS Version	Download Loc	Homepage	License	Path within the Package to be disclosed
325423	SRC	Glib		https://ftp.gnome.org	URL	LGPL-2.1	/glib

Package File

[glib \(3\).zip](#)

Path or File

Notice Type : General

License	
FTL	Copyright (c) 2006-2011 by Daniel Lemberg.
Apache-2.0	

4단계 : Distribution (Software 승인)

❑ OSS 고지문구 및 공개할 Source Code (Package)를 OSS 배포사이트에 등록

← → ↻ opensource.lge.com/index

앱 ★ Bookmarks 장학생S - 보고및... 회의실예약 Bible4U - Online B... lap [MC Lab Wiki] Port Access | Port... BASH FAQ

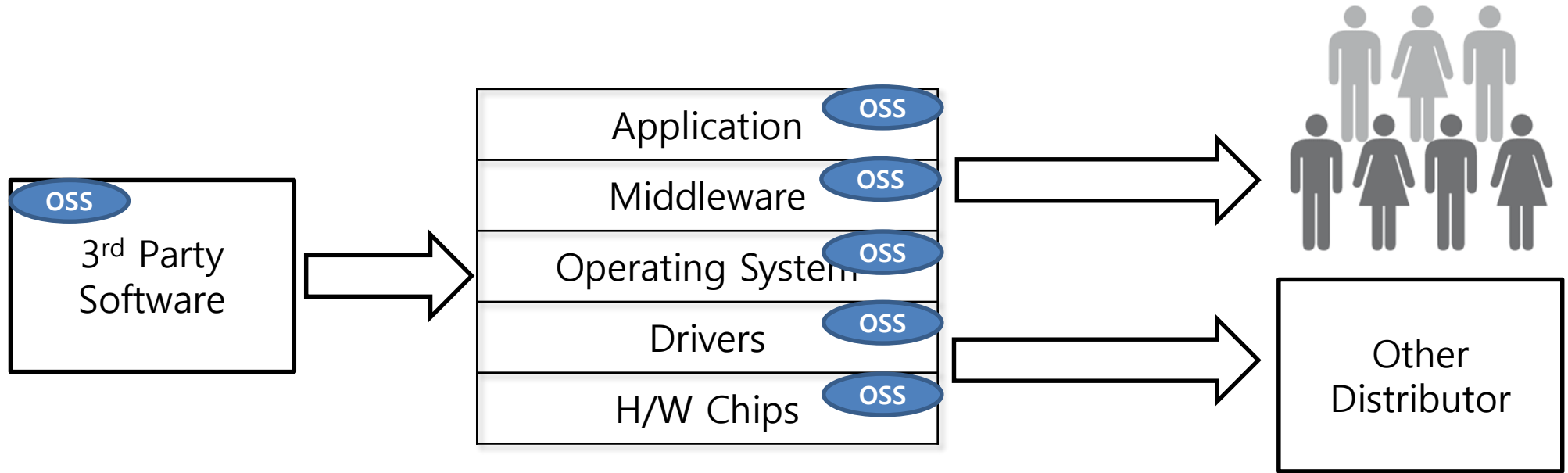
OpenSource Code Distribution

AV/Car/Security	Appliances	Commercial	Computer Product	Mobile	TV/Display	ETC
ALL AV/Car/Security Car Infotainment Media Player Security VCS	ALL Appliances Air Conditioner Cooking Machine Refrigerator Vacuum Cleaner Washing Machine	ALL Commercial BdMS Business Comm. Head-End Systems Solar	ALL Computer Product Data Storage PC & Laptop PC Accessory	ALL Mobile Mobile Phone Modem Tablet	ALL TV/Display LCD Monitor/Signage PDP Projector	ALL ETC Common Etc

The open source software and source code are provided to you on an "AS IS" basis and LGE, its affiliates and subsidiaries disclaim any and all warranties and representations with respect to such software and related source code, whether express, implied, statutory or otherwise, including without limitation, any implied warranties of title, non-infringement, merchantability, satisfactory quality, accuracy or fitness for a particular purpose.

Software 공급망 관리

Open Source is everywhere



3rd Party Software 계약

▪ (예) 표준계약서 내 Open Source 관련 보증 조항

3. “목적물”에 Open Source License가 적용되는 소프트웨어가 포함된 경우, “회사”는 (i) 첨부(6) Open Source License 관련 약사항을 철저히 준수하고, (ii) 첨부(7) Open Source Software List를 사실대로 정확히 기재하여 “LG전자”에게 “목적물”을 인도하는 시점에 함께 제출해야 한다. Open Source License란, (i) 소프트웨어 개발자에게 자신의 소프트웨어나 그 부속물에 관하여 의무사항이 발생하게 하거나, (ii) 소프트웨어 개발자 자신의 소프트웨어나 그 부속물에 관한 지적재산권 상의 권리를 제3자에게 허여하도록 하는 소프트웨어 라이선스를 뜻한다. 대표적인 Open Source License로는 GNU General Public License나 GNU Lesser General Public License 등이 있다. ㄴ
4. 본조의 보증에 대한 위반이 발생하는 경우, “회사”는 자신의 비용과 책임으로 “목적물 등”의 수정, 교환 등을 포함하여 가능한 모든 수단과 방법을 다하여 그 하자를 치유하여야 하며, 이로 인하여 “LG전자” 또는 제3자가 손해를 입은 경우에는 그 손해를 모두 배상하여야 한다. ㄴ

계약발생신고/검토요청

 도움말

위 계약에 소프트웨어가 포함되어 있다면, 오픈소스 소프트웨어도 포함되어 있습니까?

☐ Yes/잘모르겠음 ☐ No

※ 필수항 계약경고 관공인

[TEST]

임시저장

취소

3rd Party OSS Checklist

Checklist

Checklist	Agreement
0. Open Source가 사용되지 않는다는 진술 공급사는 공급 Software내 Open Source가 사용되지 않는다고 선언한다.	
1. LG전자에게 소프트웨어를 전달할 경우 LG전자의 오픈 소스 리스트 양식(Open Source List Sheet)에 따라 리스트를 전달하며, 1.1~1.2의 내용을 따른다.	
1.1 오픈 소스 리스트의 작성은 해당 양식의 작성 가이드를 따른다.	
1.2 오픈 소스 분석에 사용한 공식적인 방법을 명시하고 분석결과서를 제공해야 한다. (ex. Protex, Palamida, Fossology, CodeEye 등)	

OSS List

No	Binary Name or (if delivery form is source code) Source Path	OSS Name	OSS Version	License	Download Location	Homepage	Copyright Text	License Text	Modified or not
	[Binary Name 혹은 (delivery form이 Source Code인 경우) Source Path]	[사용한 OSS 이름]	[OSS의 Version]	[OSS의 License, SPDX Identifier (https://spdx.org/licenses/) 형태로 기입]	[OSS를 Download 받을 수 있는 URL 혹은 VCS location]	[OSS의 홈페이지]	[OSS의 Copyright 정보. 예: Copyright (c) 2017 LG Electronics.]	[License 전문, License를 SPDX Identifier로 기입한 경우, 생략 가능]	[OSS를 수정한 경우, "Modified"로 기입]
1									
2									
3									

Compliance Activities

Claim Response System

❑ Open Source와 관련된 외부 요청이 접수되면 가능한 빠른 시간 내에 대응

○ Your Inquiry list

Total inquiry	12	Ongoing	2	Delay	0
---------------	----	---------	---	-------	---

No	State	Type	Category	SubCategory	Model	Customer	Division	Inquiry Date	Reply Date	Comment
1	 new	N/A	TV/Display	LCD			N/A	2014.12.24	-	N
2	 new	N/A	Mobile	Mobile Phone			N/A	2014.12.23	-	N
3	 new	N/A	TV/Display	Monitor/Signage			N/A	2014.12.23	-	N
4	 new	N/A	TV/Display	Monitor/Signage			N/A	2014.12.23	-	N
5	 new	N/A	TV/Display	Monitor/Signage			N/A	2014.12.23	-	N
6	 new	OSSUpload	Computer Product	Data Storage			CTO>CI Center	2014.12.23	-	Y
7	 new	OSSUpload	Commercial	Head-End Systems			CTO>SW Platform Lab.	2014.12.23	-	N
8	 new	N/A	AV/Security	Security			N/A	2014.12.23	-	N
9	 new	N/A	AV/Security	Security			N/A	2014.12.23	-	N
10	 new	N/A	Mobile	Mobile Phone			N/A	2014.12.22	-	N

Training

□ 국내 및 해외 Software 개발자 대상 주기적인 Open Source License 교육 진행



Online Training

□ Online 교육 과정 제공 (기본과정 / 심화과정 구분)

- 플래시 애니메이션 형태의 교육으로 오픈소스 라이선스에 대해 쉽게 설명
- LG전자 임직원이 필수적으로 알아야 할 오픈소스 관리 프로세스의 이해



Open Source Compliance Workshop

□ 매 분기 각 사업부 OSC 담당자 대상 Open Source Compliance Workshop 개최

20th Open Source Compliance Workshop

일자 : 2017. 6. 27
 시간 : 오후 1시 30분 ~ 오후 5시
 장소 : 양재 R&D (구) 우면캠퍼스 2층 대회의실

시간	주제	발표자
13:30 - 13:40	Opening Talk	
13:40 - 14:00	Binary Analysis	
14:00 - 14:30	Open Chain과 SPDX	
14:30 - 14:50	Coffee Break	
14:50 - 15:10	OSC System 개선 사항	
15:10 - 15:30	Process 개선 사항	
15:30 - 15:50	외부 Claim 대응 사례	
15:50 - 16:10	Coffee Break	
16:10 - 16:25	캐나다항 번역 관련 이슈 공유	
16:25 - 17:00	사업부간 토론	

19th Open Source Compliance Workshop

일자 : 2017년 3월 28일 (화)
 시간 : 오후 1시 30분 ~ 오후 5시
 장소 : 서초 R&D 캠퍼스 타워동 14층 교육실 2

시간	발표자	주제
13:30 - 13:40		Opening Talk
13:40 - 14:10		Compliance Risk Prevention Activity
14:10 - 14:50		Open Source Compliance Update
14:50 - 15:10		Coffee Break
15:10 - 15:30		Android Binary Analysis
15:30 - 16:00		VC Best Practice
16:00 - 16:10		Coffee Break
16:10 - 16:40		Open Source License Question Cases
16:40 - 17:00		CAV Issue 공유

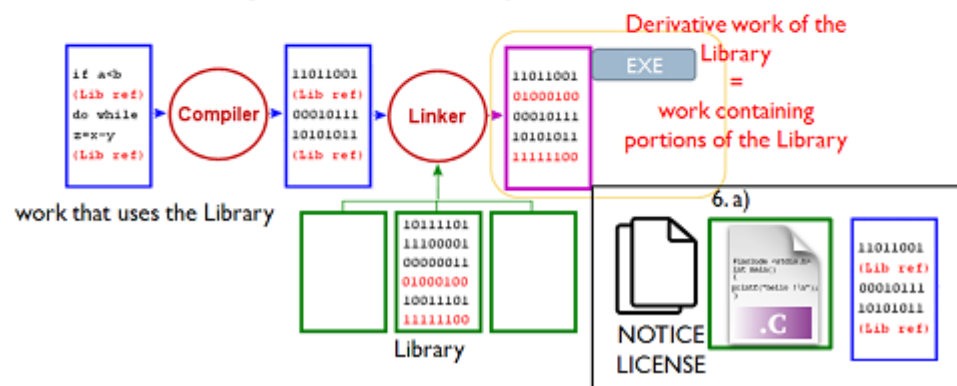


Open Source License Forum

□ 세미나 형태의 Open Source License Study forum 진행

LGPL 2.1 - Section 6.

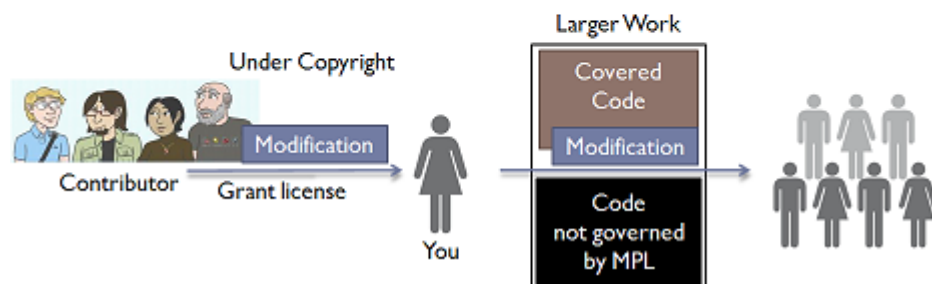
- ▶ and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library.



2. Source Code License

2.2. Contributor Grant.

(a) under intellectual property rights (other than patent or trademark) Licensable by Contributor, to use, reproduce, modify, display, perform, sublicense and distribute the Modifications created by such Contributor (or portions thereof) either on an unmodified basis, with other Modifications, as Covered Code and/or as part of a Larger Work; and



Open Source Newsletter

❑ Open Source 관련 동향 및 사내 이슈를 newsletter 형식으로 격월 발행



Open Source Newsletter

English

April 2016 (46호)

오픈 소스 관련 이슈 및 동향에 관한 사내외 정보를 전달 드리기 위해 격월로 발행합니다.

"2016년부터 Open Source Newsletter의 수신자를 전직원으로 확대하였습니다.
오픈 소스와 관련한 사내외 유용한 정보를 전달해 드리겠습니다."

주요 소식

2016 전사 Risk 예방 활동 : Open Source



LG전자 모든 사업부는 Compliance Risk 예방 및 실질적 개선을 위해 매년 전사적으로 실시하는 "Risk 예방활동"을 이행하고 있으며, Open Source는 중점 관리가 필요한 13개 Risk 중 하나입니다. 준법감시팀에서 2016년도 Risk 예방활동 실시에 대해 5월 중 공지 예정이며, Open Source 관련 세부 이행 방법에 대해서 사업부 Open Source 담당자에게 별도로 안내 드리겠습니다.

❑ 전 사업부에서 Open Source를 사용하면서 준수해야 할 사항에 대해 설명



COLLAB

Spaces ▾

People

Questions

Calendars

Browse ▾

Create

Search

FOSS Home

Created by 전상용 sangyongjeon, last modified by 박원재 wonjae.park on 2017/06/14

Korean English

이 공간은 LG 전자에서 Open Source Software를 사용하면서 준수하여야 할 의무사항에 대해 자세히 설명합니다.

NOTICE

[17/06/15] OSS 안내문구 보완

[17/06/15] Binary 분석 방법 보완

[17/06/15] OSS 고지방법 보완 - 간소화된 OSS 고지문구 지원

[17/06/12] Android Binary 분석 script update : v3.08

[17/05/30] 전자 Open Source Compliance 표준 프로세스 개정

[17/05/29] Artifex v. Hancom (한컴) 소송 사례

[17/05/02] [BOOK] Practical GPL Compliance

[17/04/17] GPL Font Exception

[17/04/09] Android Binary 분석 script update : v3.07

[17/03/31] GPL과 Bootloader (U-Boot exception)

31 related results

more

QUICK LINK

1. 3rd Party Software 관리 (계약서 / 3rd Party OSS Checklist)

2. Source Code 분석 (FOSSology / Protex)

3. Binary 분석

4. OSS 보고서

5. OSS 고지문구 / OSS 안내문구

6. OSS 고지 방법

7. 공개할 Source Code취환

CHILD PAGES

Expand all Collapse all

NOTICE

0. 조직별 OSC 담당자 현황

OSC 담당자 역할 및 Compliance 활동

1. Open Source License

1.1. Overview

1.2. License List

1.3. 소송/위반 사례

1.4. License 확인 방법

1.5. License FAQ

1.6. 주요 소프트웨어 License

2. Open Source Compliance

2.1. OSC Process

2.2. 개발/배포 형태별 요구사항

2.3. 3rd Party Software 관리

2.4. 외부 클레임 대응

2.5. 표준 OSC Process 문서

2.6. Risk 예방활동

2.7. Android 기반 모델

3. Open Source Governance

3.1. Open Source Contribution Process

3.2. Open Source 보안 취약점

4. System & Tools

4.1. CLM - OSC

4.2. Protex - Code Scanning Tool

4.3. OSC System

4.4. OSS Distribution Site

4.5. Other Compliance Tools

4.6. FOSSology - Code Scanning Tool

Copy of 2.4. 외부 클레임 대응-Draft version

3. Open Source Governance

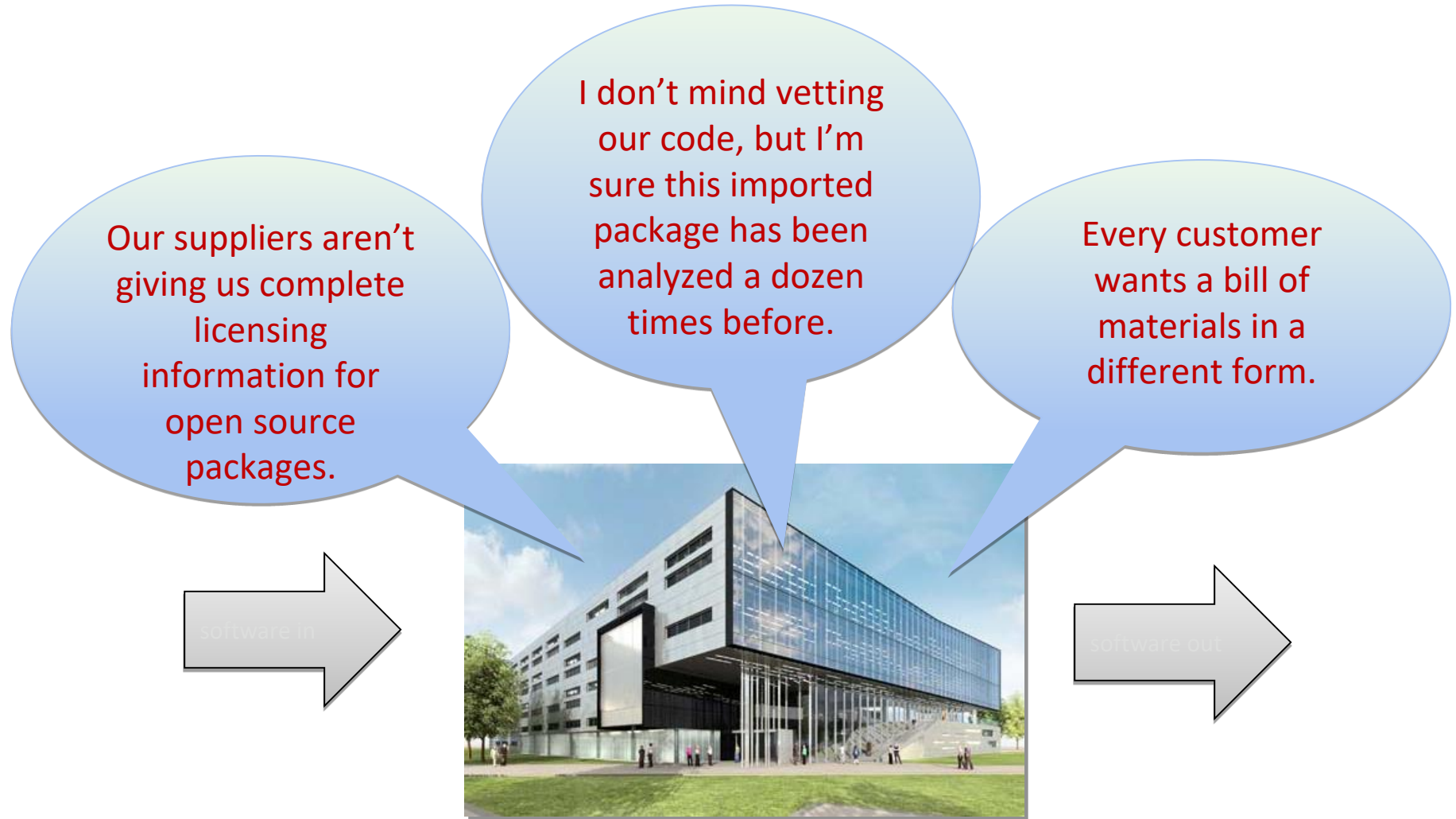
25 / 48

Open Source Community Tool 활용

1. SPDX

Software 정보 교환 방식의 표준화 필요 :

❑ SPDX (Software Package Data Exchange)



<https://spdx.org/>

SPDX License List

❑ License 이름 표준화 : <http://spdx.org/licenses/>

Version: 2.6 6 Jan 2017

Note: You can sort by each column by clicking on the column header.

Full name	Identifier	OSI Approved?	Text
3dfx Glide License	Glide		License Text
Abstyles License	Abstyles		License Text
Academic Free License v1.1	AFL-1.1	Y	License Text
Academic Free License v1.2	AFL-1.2	Y	License Text
Academic Free License v2.0	AFL-2.0	Y	License Text
Academic Free License v2.1	AFL-2.1	Y	License Text
Academic Free License v3.0	AFL-3.0	Y	License Text
Academy of Motion Picture Arts and Sciences BSD	AMPAS		License Text
Adaptive Public License 1.0	APL-1.0	Y	License Text
Adobe Glyph List License	Adobe-Glyph		License Text
Adobe Postscript AFM License	APAFML		License Text
Adobe Systems Incorporated Source Code License Agreement	Adobe-2006		License Text
Affero General Public License v1.0	AGPL-1.0		License Text
Afmparse License	Afmparse		License Text
Aladdin Free Public License	Aladdin		License Text
Amazon Digital Services License	ADSL		License Text
AMD's plpa_map.c License	AMDPLPA		License Text
ANTLR Software Rights Notice	ANTLR-PD		License Text
Apache License 1.0	Apache-1.0		License Text
Apache License 1.1	Apache-1.1	Y	License Text
Apache License 2.0	Apache-2.0	Y	License Text

SPDX License Identifiers in Source

[projects](#) / [u-boot.git](#) / blob

[\[u-boot.git\]](#) / [post](#) / [post.c](#)

```
1 /*
2  * (C) Copyright 2002
3  * Wolfgang Denk, DENX Software Engineeri
4  *
5  * SPDX-License-Identifier:    GPL-2.0+
6  */
7
8 #include <common.h>
9 #include <stdio_dev.h>
10 #include <watchdog.h>
11 #include <div64.h>
12 #include <post.h>
13
14 #ifdef CONFIG_SYS_POST_HOTKEYS_GPIO
15 #include <asm/gpio.h>
16 #endif
17
18 #ifdef CONFIG_LOGBUFFER
19 #include <logbuff.h>
20 #endif
21
22 DECLARE_GLOBAL_DATA_PTR;
```

 [projects](#) / [lmg](#) / [odp.git](#) / blob

[\[lmg/odp.git\]](#) / [include](#) / [odp.h](#)

```
1 /* Copyright (c) 2013, Linaro Limited
2  * All rights reserved
3  *
4  * SPDX-License-Identifier:    BSD-3-Clause
5  */
6
7 /**
8  * @file
9  *
10 * The OpenDataPlane
11 *
12 */
13
14 #ifndef ODP_H_
15 #define ODP_H_
16
17 #ifdef __cplusplus
18 extern "C" {
```

 [pocoproject](#) / [poco](#)

Branch: [develop](#) [poco](#) / [Util](#) / [src](#) / [ConfigurationMapper.cpp](#)

104 lines (81 sloc) | 2.27 KB

```
1 //
2 // ConfigurationMapper.cpp
3 //
4 // $Id: //poco/1.4/Util/src/ConfigurationMapper.cpp#1 $
5 //
6 // Library: Util
7 // Package: Configuration
8 // Module: ConfigurationMapper
9 //
10 // Copyright (c) 2004-2006, Applied Informatics Software Engineering GmbH.
11 // and Contributors.
12 //
13 // SPDX-License-Identifier:    BSL-1.0
14 //
15
16
17 #include "Poco/Util/ConfigurationMapper.h"
18
19
20 namespace Poco {
21 namespace Util {
```



Search

Specifications

The following are the SPDX specifications past, present and future.

- To see a current list of issues you can [access our bugzilla database](#). To enter a bug on the specification you may need to get an account on the Linux Foundation Bugzilla system (it's free).
- If you have questions about the specification you can ask them on the [technical team mailing list](#).
- If you are not subscribed to the technical team mailing list [sign up here](#). You will need to subscribe to be able to send an email to the list.

Current Version

SPDX Document Version	Formats			
2.1	PDF	HTML	RDF	OWL

Previous Versions

SPDX Document Version	Formats			
2.0	PDF	RDF (archive)	OWL	

SPDX v2.1 Document contains:

Document Creation Information

Package Information

File Information

Snippet Information

Other Licensing Information

SPDX Documents

```
##-----  
## Package Information  
##-----
```

```
PackageName: time-1.7.tar.gz  
PackageFileName: time-1.7.tar.gz  
PackageDownloadLocation: NOASSERTION  
PackageVerificationCode: dd5cf0b17bfef4284c6c22471b277de7beac407c  
PackageChecksum: SHA1: dde0c28c7426960736933f3e763320680356cc6a  
PackageLicenseConcluded: GPL-2.0+  
PackageLicenseDeclared: GPL-2.0+
```

```
PackageLicenseInfoFromFiles:  
PackageLicenseInfoFromFiles:  
PackageLicenseInfoFromFiles:  
PackageLicenseInfoFromFiles:  
PackageLicenseInfoFromFiles:  
PackageLicenseInfoFromFiles:  
PackageCopyrightText: NOASSER
```

```
##-----
```

```
- <rdf:Description rdf:nodeID="A0">  
  <rdfs:comment/>  
  - <copyrightText>  
    * <I>Copyright</I> (C) 1999 by Randolph Chung &lt;tausq@debian.org>;  
  </copyrightText>  
  <licenseComments/>  
  <licenseInfoInFile rdf:resource="http://spdx.org/licenses/GPL-2.0+"/>  
  <licenseConcluded rdf:resource="http://spdx.org/rdf/terms#noassertion"/>  
  <fileType rdf:resource="http://spdx.org/rdf/terms#fileType_source"/>  
  <checksum rdf:nodeID="A1"/>  
  <fileName>networking/hostname.c</fileName>  
  <rdf:type rdf:resource="http://spdx.org/rdf/terms#File"/>  
</rdf:Description>  
- <rdf:Description rdf:nodeID="A2">  
  <checksumValue>dc90a437e03f31ab04e7059d8da5f88b28cde77d</checksumValue>  
  <algorithm rdf:resource="http://spdx.org/rdf/terms#checksumAlgorithm_sha1"/>  
  <rdf:type rdf:resource="http://spdx.org/rdf/terms#Checksum"/>  
</rdf:Description>  
- <rdf:Description rdf:nodeID="A3">  
  <rdfs:comment/>  
  <copyrightText rdf:resource="http://spdx.org/rdf/terms#none"/>  
  <licenseComments/>
```

SPDX Group이 제공하는 spreadsheet template

Home Layout Tables Charts SmartArt Formulas Data Review						
Edit Paste Fill Clear Font Arial 10 A A B I U Alignment abc Wrap Text Number General % 0.00						
P123 fx						
	A	B	C	D	E	
1	6.1 File Name	6.2 File Type	6.3 File Checksum	6.4 License Concluded	6.5 License Info in File	6.6 L
2	time-1.7\AUTHORS	OTHER	7951F4CEFFDB030EC617ED DF7BBA22523CC1A67F	NOASSERTION	NONE	
3	time-1.7\ChangeLog	OTHER	4A972EE2C972E38B502B228 37C2513ECC2647339	NOASSERTION	NONE	
4	time-1.7\configure	OTHER	A54A5E0A7321967322E7E71 A5F0E23B59F2BBB15	LicenseRef-3	LicenseRef-3	
5	time-1.7\configure.in	OTHER	63F77F68E8E90B3E6FDDE4 BE3B585B72A0635B8F	NOASSERTION	NONE	
6	time-1.7\COPYING	OTHER	075D599585584BB0E4B526F 5C40CB6B17E0DA35A	GPL-2.0	GPL-2.0	
7	time-1.7\error.c	SOURCE	97BFD964AAE09D71B7FA89 BD48B2110CB8D3E12D	GPL-2.0+	GPL-2.0+	
8	time-1.7\getopt.c	SOURCE	4EEC2F371CDEA3FA5F96A3 7B44B200445609BC75	GPL-2.0+	GPL-2.0+	
9	time-1.7\getopt.h	SOURCE	512169AACCC1C0FE20D E76AF4A5FF347AAC05	GPL-2.0+	GPL-2.0+	
10	time-1.7\getopt1.c	SOURCE	177C2F08AAD7203FA875AE6 3C0EC92FBB3C9F600	GPL-2.0+	GPL-2.0+	
11	time-1.7\getpagesize.h	SOURCE	1EF18700B72387BF6322695 BB1AEC2CA5E18CB00	NOASSERTION	NONE	
12	time-1.7\INSTALL	OTHER	BD0CE8678F58293AFC2069 E6BA9AB42A6C3E23BC	NOASSERTION	NONE	
13	time-1.7\install-sh	SOURCE	C5C249A2DD763530AE65D2 8BC1C64BB754CD0750	MIT	MIT	
14	time-1.7\Makefile.am	SOURCE	013F7D712AEFD2409A23107 14257AD77E62CA205	NONE	NONE	
15	time-1.7\Makefile.in	SOURCE	8B548F3A4C3719B30E0A5D B65DD53ADBDA180DB0	LicenseRef-2	LicenseRef-2	
16	time-1.7\mdate-sh	SOURCE	7A4FCB88FD92B03E9DD69F 04DBA7ED442B33086C	GPL-2.0+	GPL-2.0+	
17	time-1.7\mkinstalldirs	OTHER	8BC81B299F7F9A483A21AE3 6C7A5661D832974EF	INTHEPUBLICDOMAIN	INTHEPUBLICDOMAIN	
18	time-1.7\NEWS	OTHER	9A94D3FD8BE03E1947B8C4 3DE83211FE4F8EA38C	NOASSERTION	NONE	
19	time-1.7\port.h	SOURCE	966E3DC7BAE8B140BEDC52 D8F3AB3A87F1815656	NOASSERTION	NONE	
2.0 Doc Info 3.0 Creation Info 4.0 Package Info 5.0 Other Licensing 6.0 File Info 7.0 Reviewer Info +						

SPDX Workgroup Tool : Converter / Viewer / Compare

❑ Command line interface tool (jar)

```
$ java -jar spdx-tools-jar-with-dependencies.jar <function> <parameters>
```

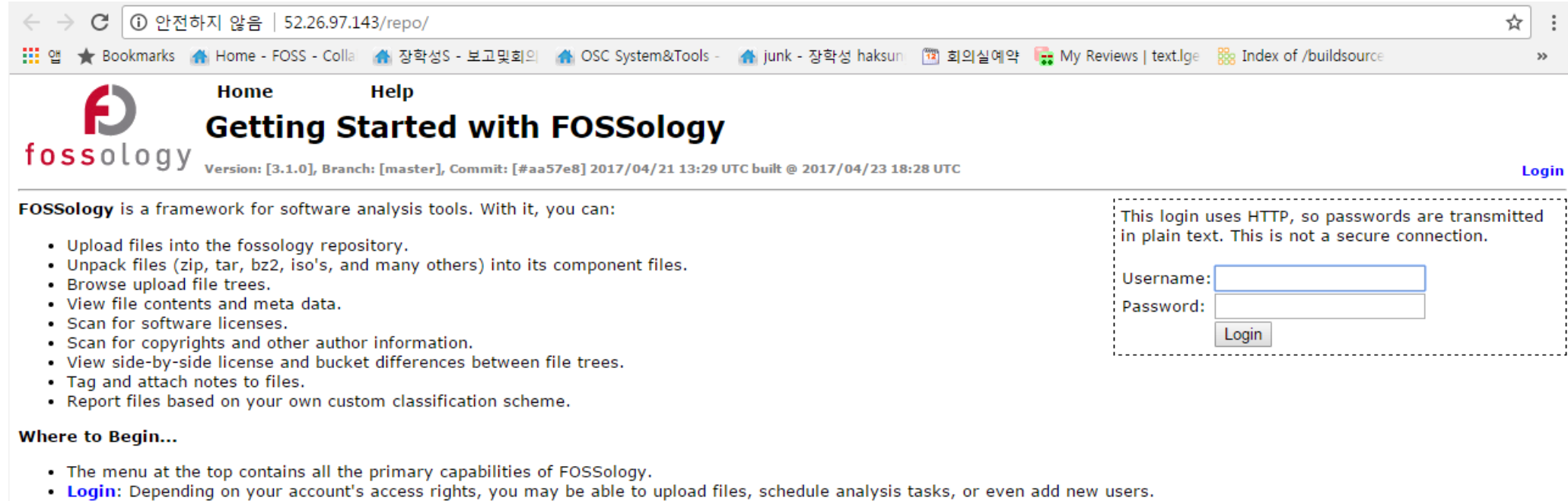
category	functions	parameters	descriptions
converter	TagToSpreadsheet	inputFile outputFile	convert : tag format -> spreadsheet
	TagToRDF	inputFile outputFile	convert : tag format -> RDF
	RdfToTag	inputFile outputFile	convert : RDF -> tag format
	RdfToHtml	inputFile outputFile	convert : RDF -> HTML
	RdfToSpreadsheet	inputFile outputFile	convert : RDF -> spreadsheet
	SpreadsheetToRDF	inputFile outputFile	convert :spreadsheet -> RDF
	SpreadsheetToTag	inputFile outputFile	convert : spreadsheet -> tag format
Viewer	SPDXViewer	inputFile	Display an SPDX document input file
Compare	CompareSpdxDocs	output.xls doc1 doc2 ... docN	Compare two SPDX documents
	CompareMultipleSpdxDocs	doc1 doc2 [output]	Compare multiple SPDX documents

Open Source Community Tool 활용

2. FOSSology

What is FOSSology?

- ❑ Web server application for license and copyright compliance of software components.



The screenshot shows the FOSSology web application interface. At the top, there is a browser address bar with the URL "52.26.97.143/repo/" and a security warning "안전하지 않음". Below the address bar is a navigation bar with links for "Home" and "Help". The main heading is "Getting Started with FOSSology". Below this, the version information is displayed: "Version: [3.1.0], Branch: [master], Commit: [#aa57e8] 2017/04/21 13:29 UTC built @ 2017/04/23 18:28 UTC". A "Login" link is visible in the top right corner. The main content area describes FOSSology as a framework for software analysis tools and lists its capabilities: uploading files, unpacking files, browsing upload file trees, viewing file contents and meta data, scanning for software licenses, scanning for copyrights and other author information, viewing side-by-side license and bucket differences, tagging and attaching notes to files, and reporting files based on a custom classification scheme. A "Where to Begin..." section provides additional guidance, including a link to the "Login" page. A warning box on the right side of the page states: "This login uses HTTP, so passwords are transmitted in plain text. This is not a secure connection." Below this warning, there are input fields for "Username:" and "Password:", and a "Login" button.

Home Help

Getting Started with FOSSology

Version: [3.1.0], Branch: [master], Commit: [#aa57e8] 2017/04/21 13:29 UTC built @ 2017/04/23 18:28 UTC [Login](#)

FOSSology is a framework for software analysis tools. With it, you can:

- Upload files into the fossology repository.
- Unpack files (zip, tar, bz2, iso's, and many others) into its component files.
- Browse upload file trees.
- View file contents and meta data.
- Scan for software licenses.
- Scan for copyrights and other author information.
- View side-by-side license and bucket differences between file trees.
- Tag and attach notes to files.
- Report files based on your own custom classification scheme.

Where to Begin...

- The menu at the top contains all the primary capabilities of FOSSology.
- [Login](#): Depending on your account's access rights, you may be able to upload files, schedule analysis tasks, or even add new users.

This login uses HTTP, so passwords are transmitted in plain text. This is not a secure connection.

Username:

Password:



fossology

[ABOUT](#) [FEATURES](#) [GET STARTED](#) [NEWS](#) [WIKI](#)



fossology

Open Source License Compliance by Open Source Software



ABOUT FOSSOLOGY

Learn more about FOSSology, the project governance, and license details.



GET STARTED WITH FOSSOLOGY

Instructions on how to get a local instance of FOSSology up and running from source.



IN THE NEWS

The latest announcements, news articles and events related to FOSSology.

FOSSology Installation

☐ Using docker

- <https://hub.docker.com/r/fossology/fossology/>



☐ Using vagrant & Virtual Box

- <https://github.com/fossology/fossology/wiki/vagrant>

☐ Install from source

- <https://github.com/fossology/fossology/wiki/Install-from-Source>

● Test Instance

- Server URL: <http://52.26.97.143/repo/>
- Login user name: testuser
- Login password: test

Upload OSS Package



[Home](#) [Search](#) [Browse](#) [Upload](#) [Jobs](#) [Organize](#) [Admin](#) [Help](#)

Upload a New File

Version: [3.1.0], Branch: [master], Commit: [#aa57e8] 2017/04/21 13:29 UTC built @

2017/04/23 18:28 UTC

[logout](#)

User: testuser

Group: testuser

To manage your own group permissions go into **Admin > Groups > Manage Group Users**. To manage permissions for this one upload, go to **Admin > Upload Permissions**.

This option permits uploading a single file (which may be iso, tar, rpm, jar, zip, bz2, msi, cab, etc.) from your computer to FOSSology. Your FOSSology server has imposed a maximum upload file size of 700Mbytes.

1. Select the folder for storing the uploaded files:

test-incoming777 ▼

2. Select the file to upload:

파일 선택

선택된 파일 없음

3. (Optional) Enter a description of this file:

7. (Optional) Reuse ⓘ

Select an already uploaded package for reuse in folder test-incoming777 (testuser:14) ▼

☐ enhanced reuse (slower) ⓘ

Upload to reuse:

icons-3.0.0.zip from 2017-04-25 20:42 (open)
InvoicePlane-master-2cbce741a3fc2e10cb8ad7bd01dc156f7315091d.zip from 2017-05-03 18:53 (open)
jta-1.1.jar from 2017-05-03 11:54 (in progress)
ff11.zip from 2017-05-08 09:57 (open)
ff11.zip from 2017-05-08 09:58 (open)

After you press Upload, please be patient while your file is transferring.

Upload

License Browser

← → ↻

52.26.97.143/repo/?mod=license&upload=53&item=191278

☆

📄

🔍

📁 📖 🏠 Home - FOSS - Colla 🏠 장학성S - 보고및회의 🏠 junk - 장학성 haksun 📅 회의실예약 📄 Bible4U - Online Bibl >>



Home Search Browse Upload Jobs Organize Admin Help

License Browser

Version: [3.1.0], Branch: [master], Commit: [#aa57e8] 2017/04/21 13:29 UTC built @ 2017/04/23 18:28 UTC

logout

User: testuser

Group: testuser

Folder: **test-incoming777/**
boost-1.52.0.zip

License Browser | [File Browser](#) | [Copyright/Email/URL](#) | [ECC](#) | [Browse](#) | [License List](#) | [Search](#) • [View](#) | [Info](#) • [Refresh](#)

Display licenses

Scanner Count ▾	Concluded License Count ▾	License Name ▾
1537	0	BSL-1.0
4	0	MPL
4	0	MIT-style

Showing 1 to 3 of 3 licenses

◀ Previous Next ▶

Hint: Click on the license name to search for where the license is found in the file listing.

Display files (**tree view** or **flat**)

MIT-style ▾

-- filter for edited results -- ▾

☐ on

Files ▲	Scanner Results (N: nomos, M: monk, Nk: ninka)	Edited Results	Clear Stat
boost-1.52.0	BSL-1.0, MIT-style, MPL		

Showing 1 to 1 of 1 files

Review and Adjust ("Clearing")

- ❑ Clarifying incorrect scanner results or incomplete licensing statements.
 - The scanners may find false positives.

Folder: **test-incoming777/**
boost-1.52.0.zip/boost-1.52.0/config/abi/borland_prefix.hpp
One-Shot Copyright/Email/URL • License Browser | File Browser • Info | View | Licenses | Copyright/Email/Url/Author | ECC | Bucket • Hex | Text | Formatted • Refr

Close Cleared: 0/1825

Hide Legend

```
// (C) Copyright John Maddock 2003.  
// Use, modification and distribution are subject to the  
// Boost Software License, Version 1.0. (See accompanying file  
// LICENSE_1_0.txt or copy at http://www.boost.org/LICENSE_1_0.txt)  
  
// for C++ Builder the following options effect the ABI:  
//  
// -b (on or off - effect enum sizes)  
// -Vx (on or off - empty members)  
// -Ve (on or off - empty base classes)  
// -aX (alignment - 5 options).  
// -pX (Calling convention - 4 options)  
// -VmX (member pointer size and layout - 5 options)  
// -VC (on or off, changes name mangling)  
// -VI (on or off, changes struct layout).  
  
// In addition the following warnings are sufficiently annoying (and  
// unfixable) to have them turned off by default:  
//  
// 8027 - functions containing [for|while] loops are not expanded inline  
// 8026 - functions taking class by value arguments are not expanded inline  
  
#pragma nopushoptwarn  
# pragma option push -aB -Vx- -Ve- -b- -pc -Vmv -VC- -VI- -w-8027 -w-8026
```

< Submit
>

- ☒ Go through all files ⓘ
- ☐ Go through all files with licenses ⓘ
- ☐ Go through all files with licenses and no clearing result ⓘ

Clearing decision scope

☐ Apply decision to all future occurrences of this file ⓘ

Clearing decision type

- ☐ No license known ⓘ
- ☐ To be discussed ⓘ
- ☐ Irrelevant ⓘ
- ☒ Identified ⓘ

License ⓘ ▲	Source ⓘ	Text ⓘ	Comment ⓘ	Action ⓘ
BSL-1.0	nomos: #1	Click to edit	Click to edit	✖ ⭐

Showing 1 to 1 of 1 entries

User Decision ... ⓘ Bulk Recognition ... ⓘ

Copyright Statements

Folder: [test-incoming777/](#)

[boost-1.52.0.zip](#)

[License Browser](#) | [File Browser](#) | [Copyright/Email/URL](#) | [ECC](#) | [Browse](#) | [License List](#) | [Search](#) • [View](#) | [Info](#) • [Refresh](#)

Show all ▾

Jump to: [Emails](#) | [URLs](#) | [Authors or Maintainers](#)

Show entries

Search:

[boost-1.52.0/](#)

Count ▾	Copyright ▾	
726	Copyright Aleksey Gurtovoy 2000-2004	✗
137	(C) Copyright Paul Mensonides 2002. Distributed under the Boost Software License, Version 1.0. (See accompanying file LICENSE_1_0.txt or copy at http://www.boost.org/LICENSE_1_0.txt)	✗
135	Copyright Aleksey Gurtovoy 2001-2004	✗
89	Copyright David Abrahams 2003-2004	✗
82	Copyright (C) 2001 Housemarque Oy http://www.housemarque.com	✗
61	Copyright Jaap Suter 2003	✗
60	Copyright Aleksey Gurtovoy 2003-2004	✗
53	Copyright Aleksey Gurtovoy 2002-2004	✗
39	(C) Copyright 2009-2011 Frederic Bron.	✗
33	(C) Copyright Steve Cleary, Beman Dawes, Howard Hinnant & John Maddock 2000. Use, modification and distribution are subject to the Boost Software License, Version 1.0. (See accompanying file LICENSE_1_0.txt or copy at http://www.boost.org/LICENSE_1_0.txt).	✗
26	Copyright Aleksey Gurtovoy 2004	✗

SPDX 2.0 generation

- ❑ Exporting of the Software Bill of Materials via SPDX 2.0 generation to facilitate communication in the supply chain



[Home](#) [Search](#) [Browse](#) [Upload](#) [Jobs](#) [Organize](#) [Admin](#) [Help](#)

Browse

Version: [3.1.0], Branch: [master], Commit: [#aa57e8] 2017/04/21 13:29 UTC built @ 2017/04/23

18:28 UTC

[logout](#)
User: testuser
Group: testuser

Folder

Navigation

- Expand All
- test-incoming777
 - fossology
 - Project 01
 - SubProject A
 - test01
 - test02

Shows 50 entries

Search:

Upload Name and Description	Status	Comment	Main licenses
☐ source -- select action --	open		
☐ source -- select action --	open		
☐ mkimage.zip test	open		
-- select action --	open		
-- select action --	open		
File Browser	open		
View	open		
Info	open		
Compare	open		
Copyright/Email/Url	open		
Download	open		
Export DEP5	open		
Export ReadMe_OSS	open		
Export SPDX RDF	open		
Export SPDX tag:value	open		
Licenses	open		
Tag	open		
History	open		

Open Source Community Tool 활용

3. OpenChain

What is OpenChain?

THE **LINUX** FOUNDATION PROJECTS



[News](#) [Specification](#) [Self-Certify](#) [Curriculum](#) [FAQ](#) [Community](#) [Partners](#) [Press](#)



Welcome to OpenChain

The OpenChain Project identifies key recommended processes
for effective open source management

The OpenChain Project builds trust in open source by making open source license compliance simpler and more consistent. The [OpenChain Specification](#) defines a core set of requirements every quality compliance program must satisfy. The [OpenChain Curriculum](#) provides the educational foundation for open source processes and solutions, whilst meeting a key requirement of the OpenChain Specification. [OpenChain Conformance](#) allows organizations to display their adherence to these requirements. The result is that open source license compliance becomes more predictable, understandable and efficient for participants of the software supply chain.

<https://www.openchainproject.org>



Contents

1) Introduction	3
2) Definitions.....	4
3) Requirements	5
G1: Know Your FOSS Responsibilities	5
G2: Assign Responsibility for Achieving Compliance	7
G3: Review and Approve FOSS Content.....	8
G4: Deliver FOSS Content Documentation and Artifacts.....	9
G5: Understand FOSS Community Engagement.....	10
G6: Certify Adherence to OpenChain Requirements.....	11
Appendix I: Language Translations.....	12



FOSS Training Reference Slides for the OpenChain Specification 1.1

Released under CC0-1.0.

You may use, modify, and share these slides without restriction.
They also come with no warranty.

These slides follow US law. Different legal jurisdictions may have different legal requirements.
This should be taken into account when using these slides as part of a compliance training program.

These slides do not contain legal advice

OpenChain Self-Certify

OpenChain Self Certification Survey

Specification Version 1.1 (Survey Version 1.1.0)

▼ G1: Know Your FOSS Responsibilities

8 answered out of 8

#	Question	Answer	Spec Ref
1.a:	Do you have a documented policy that governs FOSS license compliance of the Supplied Software distribution (e.g., via training, internal wiki, or other practical communication method)?	Yes ✓	1.1, 1.1.1
1.b:	Is the policy internally communicated?	Yes ✓	1.1
1.c:	Do you have a documented procedure that communicates the existence of the FOSS policy to all Software Staff?	Yes ✓	1.1.2
1.d:	Do you have FOSS training materials (e.g., slide decks or online course) covering the following topics?		1.2, 1.2.1
1.d.i:	• The FOSS policy and where to find it,	Yes ✓	1.2
1.d.ii:	• Basics of Intellectual Property law pertaining to FOSS and FOSS licenses,	Yes ✓	1.2
1.d.iii:	• FOSS licensing concepts (including the concepts of permissive and copyleft licenses),	Yes ✓	1.2
1.d.iv:	• FOSS project licensing models,	Yes ✓	1.2
1.d.v:	• Software Staff roles and responsibilities pertaining to FOSS compliance specifically and the FOSS policy in general,	Yes ✓	1.2
1.d.vi:	• Process for identifying, recording and/or tracking of FOSS components contained in Supplied Software?	Yes ✓	1.2
1.e:	Do you track the completion of the training for all Software Staff?	Yes X No	1.2.2
1.f:	Have 85% or more of the Software Staff completed a FOSS training within the last 24 months?	Yes X No	1.2; 1.2.3
1.g:	Do you have a process for reviewing the Identified Licenses to determine the obligations, restrictions and rights granted by each license?	Yes ✓	1.3
1.h:	Do you have a documented procedure to review and document the obligations, restrictions and rights granted by each license?	Yes ✓	1.3.1

► G2: Assign Responsibility for Achieving Compliance

7 answered out of 7

► G3: Review and Approve FOSS Content

3 answered out of 3

► G4: Deliver FOSS Content Documentation and Artifacts

4 answered out of 4

► G5: Understand FOSS Community Engagement

4 answered out of 4

Save Answers

Save and Submit

Download Answers

Reset

OpenChain Conformant Organizations

OpenChain Conformant Organizations



>_ ENDOCODE



GE Digital



SIEMENS



Q&A
