Open Source Governance with FOSSLight
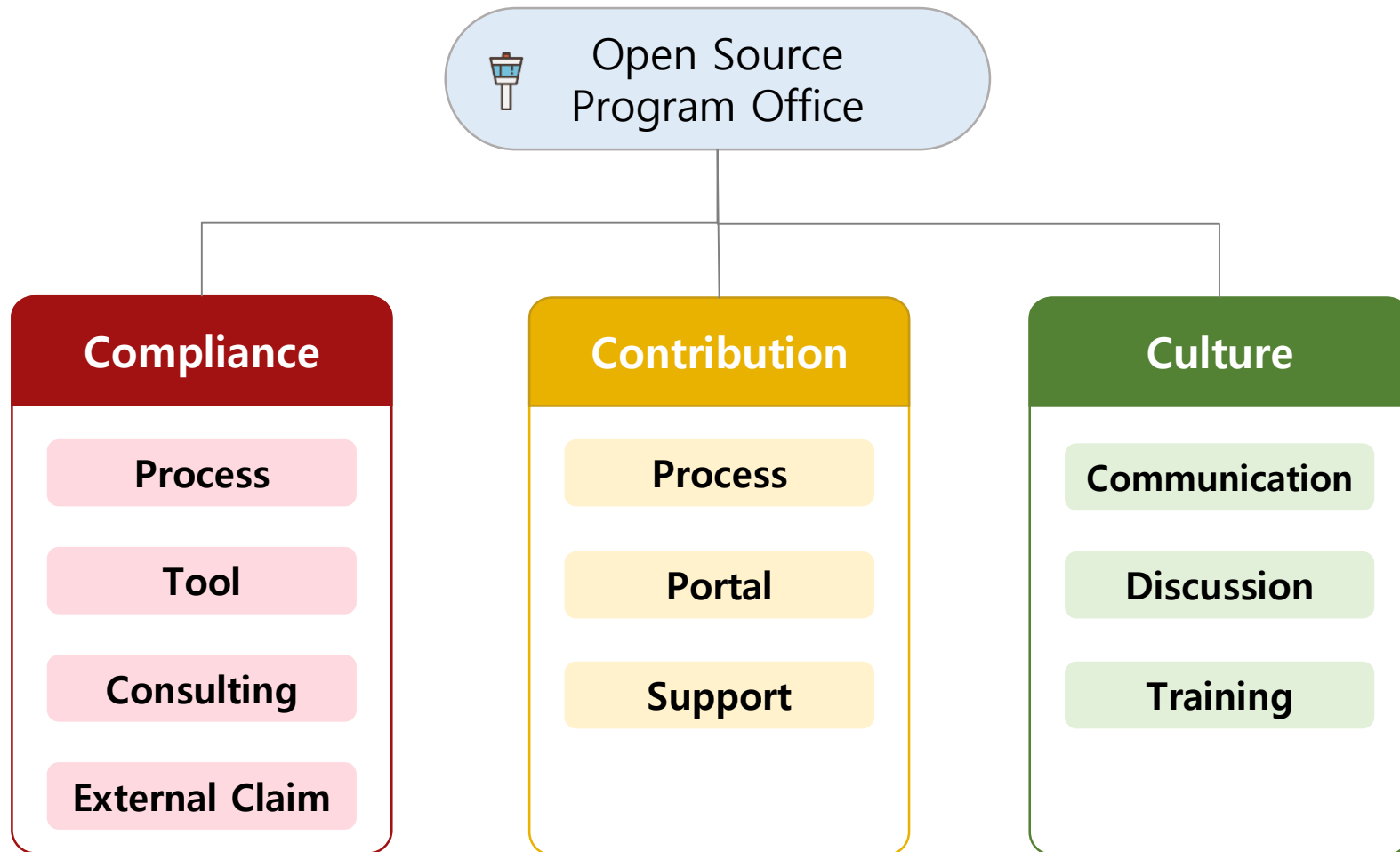
December 3, 2021

Kyoungae Kim
Open Source Task Leader
Software Center, LG Electronics
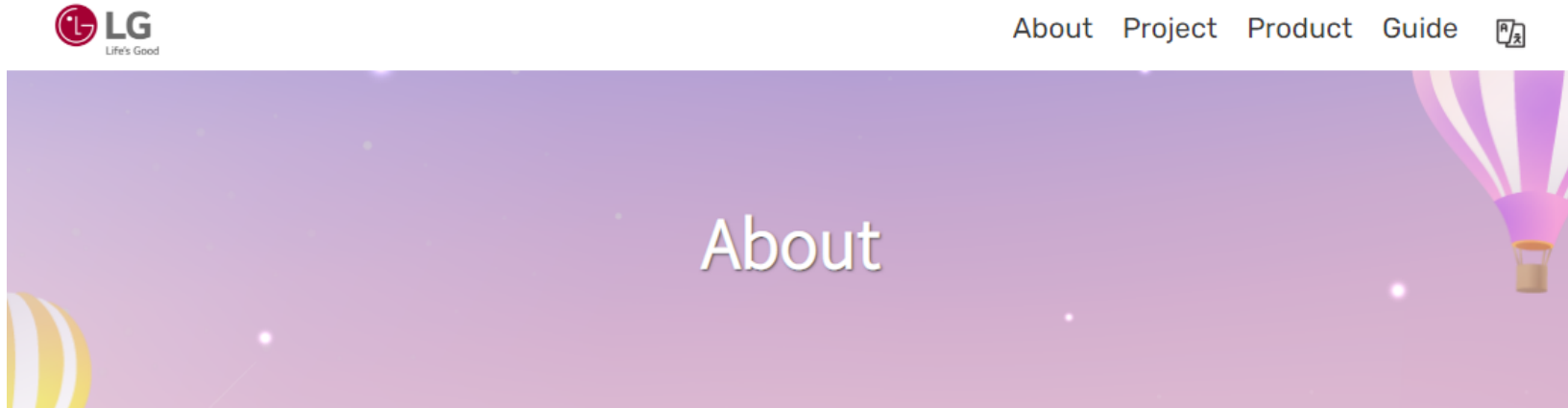
LGE Open Source Governance

Open Source Governance & Program Office

```
           ┌──────────────────────────┐
           │   Open Source            │
           │   Program Office         │
           └──────────────────────────┘
```

Compliance

- Process
- Tool
- Consulting
- External Claim

Contribution

- Process
- Portal
- Support

Culture

- Communication
- Discussion
- Training

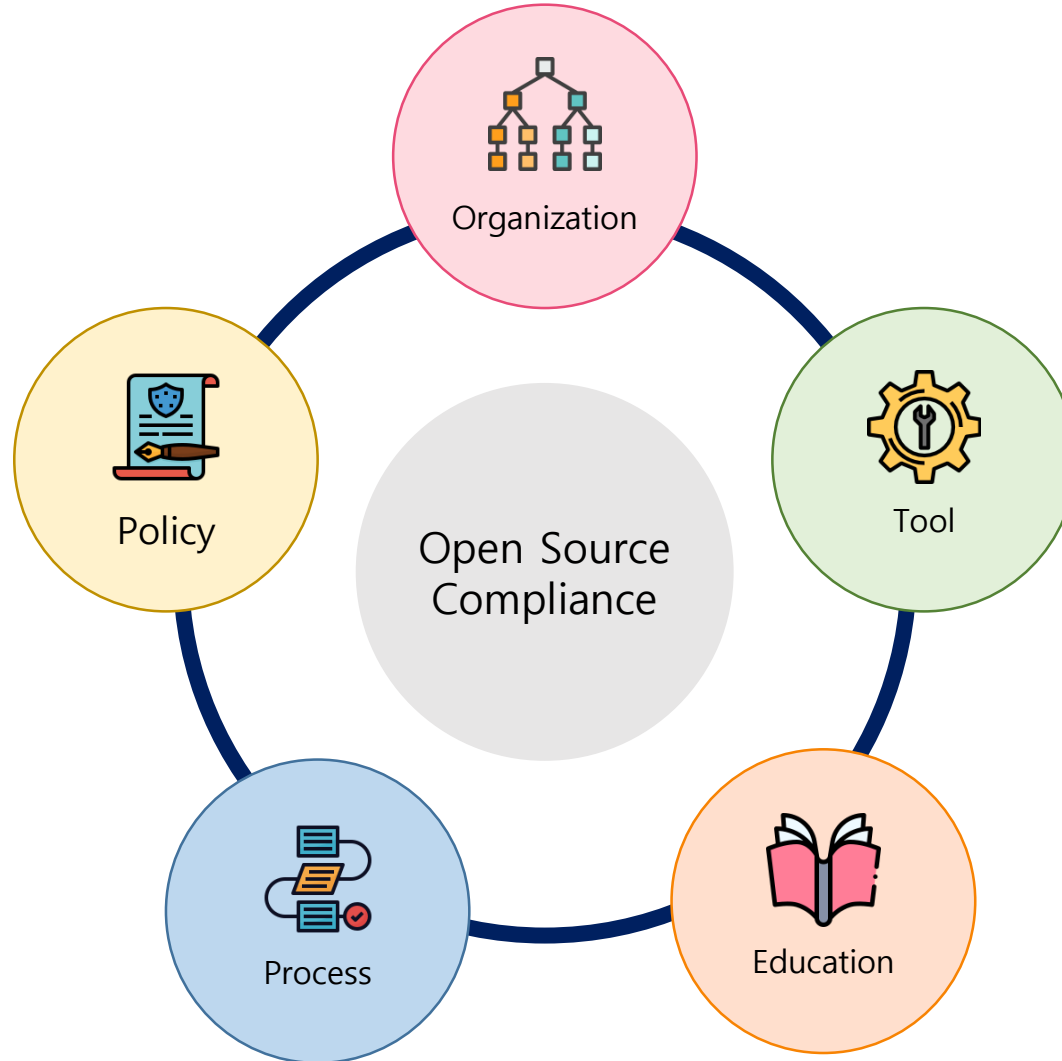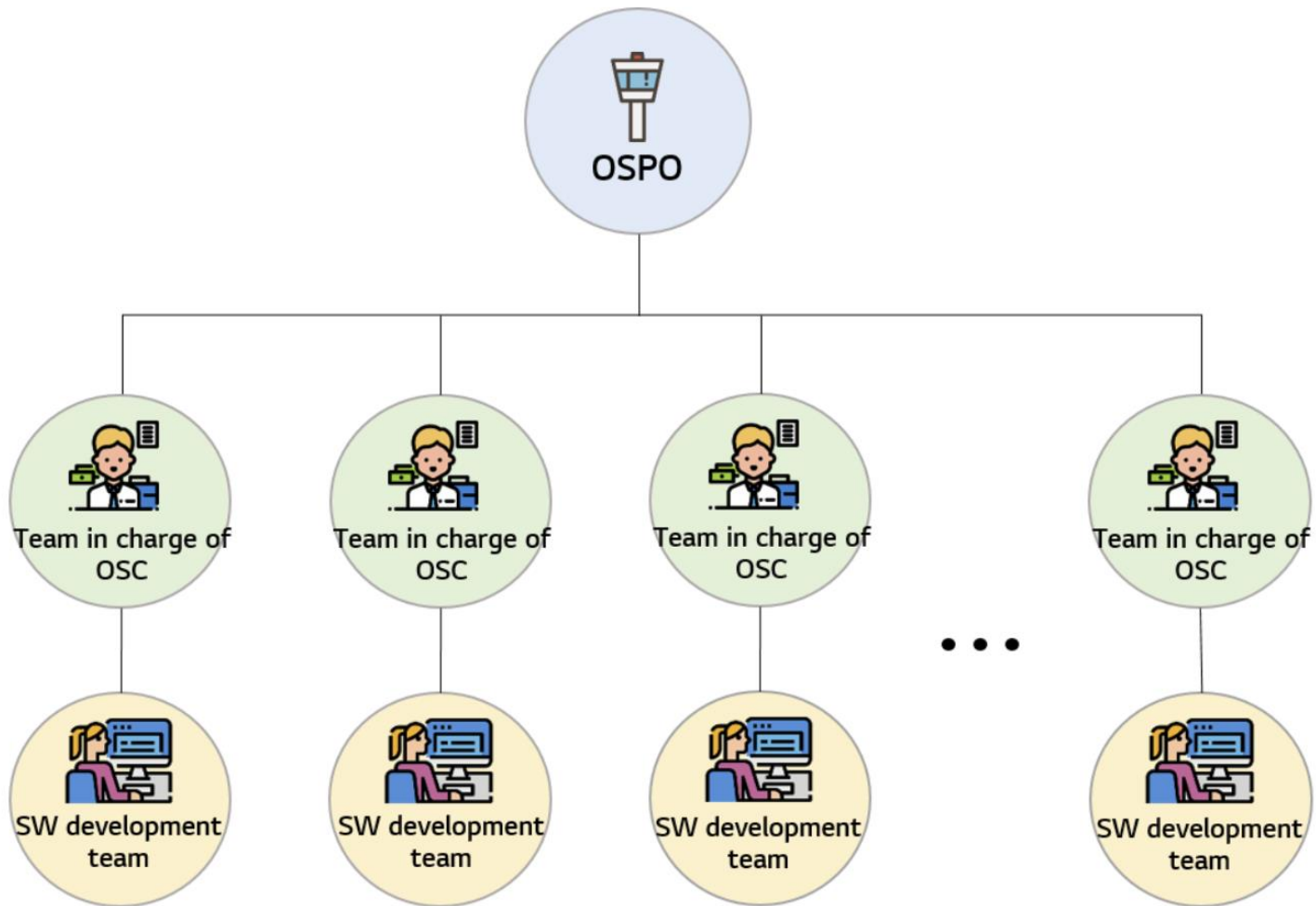https://todogroup.org/guides/create-program

Open Source Program Office

❑ **http://oss.lge.com**

LG Open Source Program Office manages open source and reduces open source compliance risk in the company. Specifically to do this, LG OSPO builds the overall open source strategy of the company such as auditing and constituting other policies on the use and distribution of open source, training for the software developers in the company, spreading an open source culture and activating participation in open source community. We disclose how LG Electronics has established an open source policy and open source compliance process in the guide page.
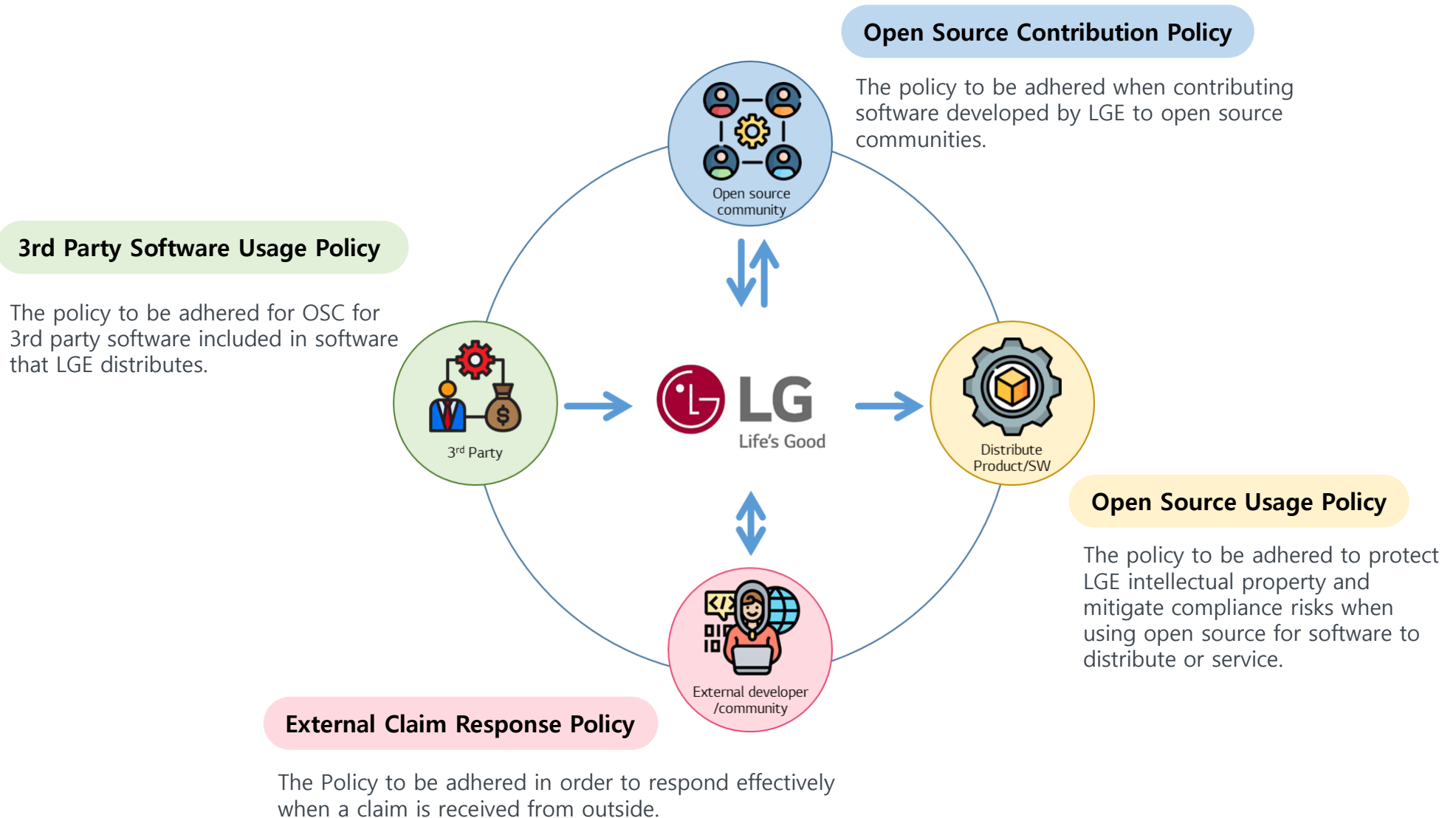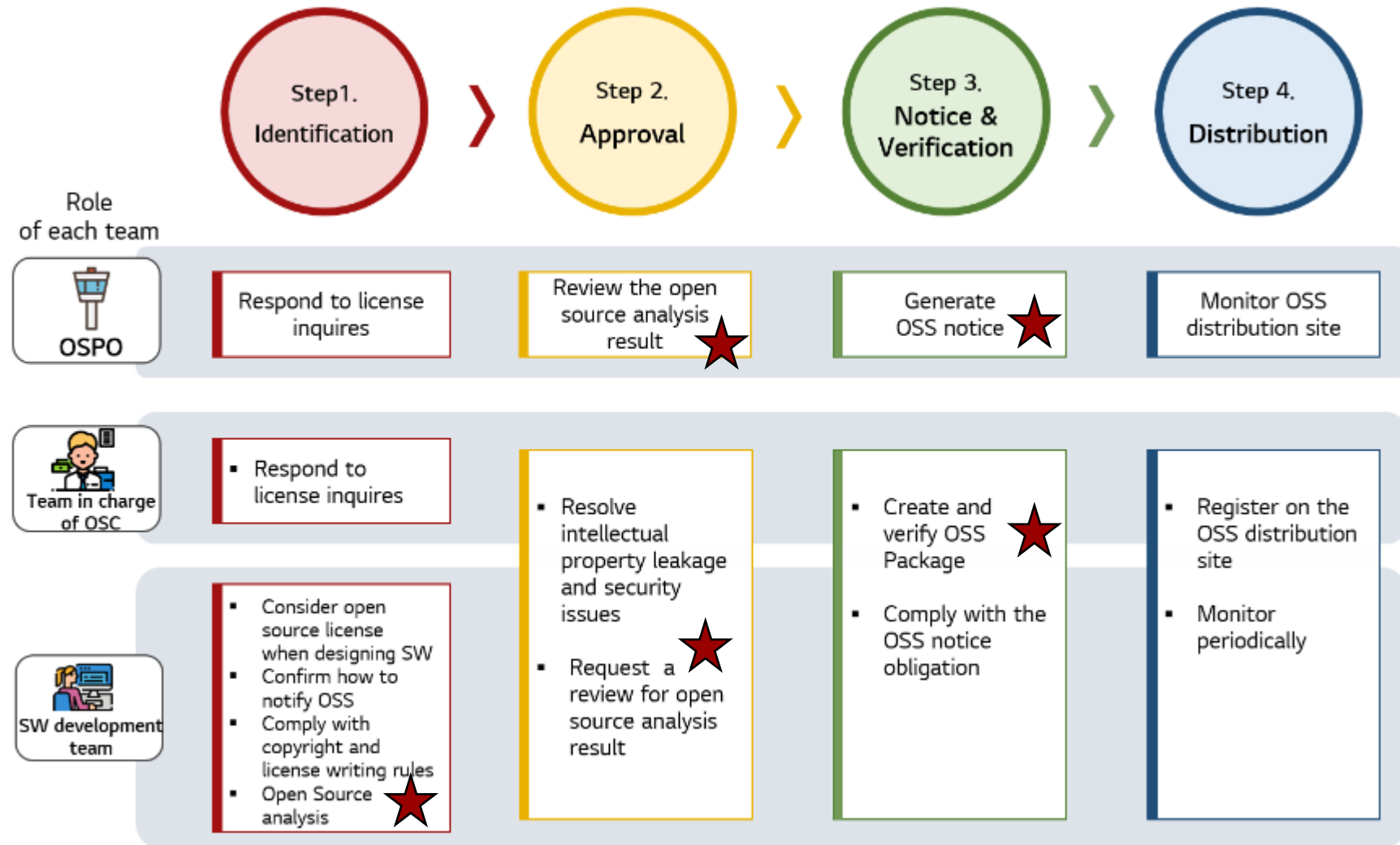
Open Source Compliance

Organization

Policy

Open Source Contribution Policy

The policy to be adhered when contributing software developed by LGE to open source communities.

3rd Party Software Usage Policy

The policy to be adhered for OSC for 3rd party software included in software that LGE distributes.

Open Source Usage Policy

The policy to be adhered to protect LGE intellectual property and mitigate compliance risks when using open source for software to distribute or service.

External Claim Response Policy

The Policy to be adhered in order to respond effectively when a claim is received from outside.

Process

Step1.
Identification

Step 2.
Approval

Step 3.
**Notice &
Verification**

Step 4.
Distribution

Role
of each team

OSPO

| Respond to license inquires | Review the open source analysis result ★ | Generate OSS notice ★ | Monitor OSS distribution site |

Team in charge of OSC

- Respond to license inquires

SW development team

- Consider open source license when designing SW
- Confirm how to notify OSS
- Comply with copyright and license writing rules
- Open Source analysis ★

- Resolve intellectual property leakage and security issues ★

- Request a review for open source analysis result

- Create and verify OSS Package ★

- Comply with the OSS notice obligation

- Register on the OSS distribution site

- Monitor periodically

Education

Education

Online training

Workshop

Video training contents

32nd
OPEN SOURCE COMPLIANCE ONLINE WORKSHOP

발표제목	발표자	시간
Introduction	김경애	14:00 ~ 14:20
LG Open Source 사이트 소개	석지영	14:20 ~ 14:30
Open Source 기여 Process 및 개발자 가이드 소개	석지영	14:30 ~ 14:50
오픈소스 툴 동향	최혜성	15:00 ~ 15:30
FOSSLight Tool 업데이트 소식	김소임	15:30 ~ 16:30
추가 문의사항 논의	김경애	16:30 ~ 17:00

2020. 09. 23 (Wed) 14:00 ~ 17:00
Join to WebEx

LGE OSC SYSTEM

Download video: mp4 format

3rd Party로부터 전달받은 Software 형태를 입력합니다.
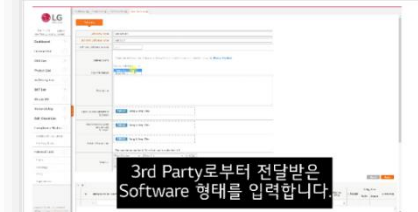
Download video: mp4 format

Download video: mp4 format

Tool

Software to be analyzed

FOSSLight Scanner

| Dependency | Source code | Binary |

OSS BOM

FOSSLight HUB

| Open Source / License Management | Compliance Process Management | Vulnerability Management |

OSS Notice

OSS distribution site

Distribute
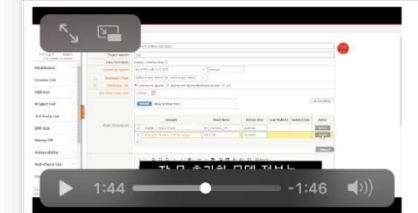
FOSSLight Open Source Project
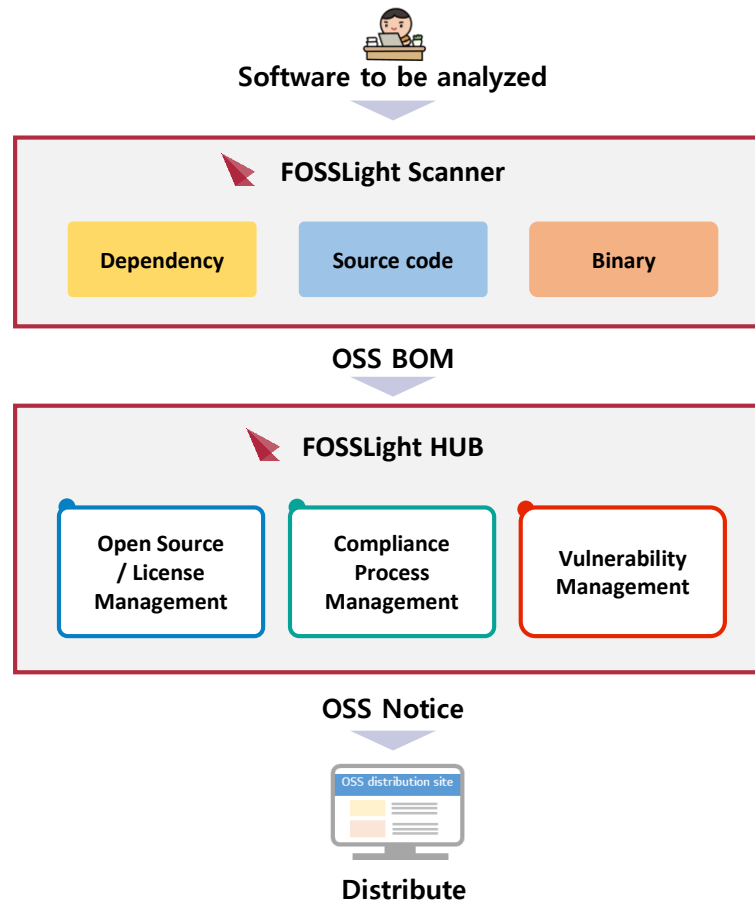
FOSSLight Project

FOSSLight Scanner
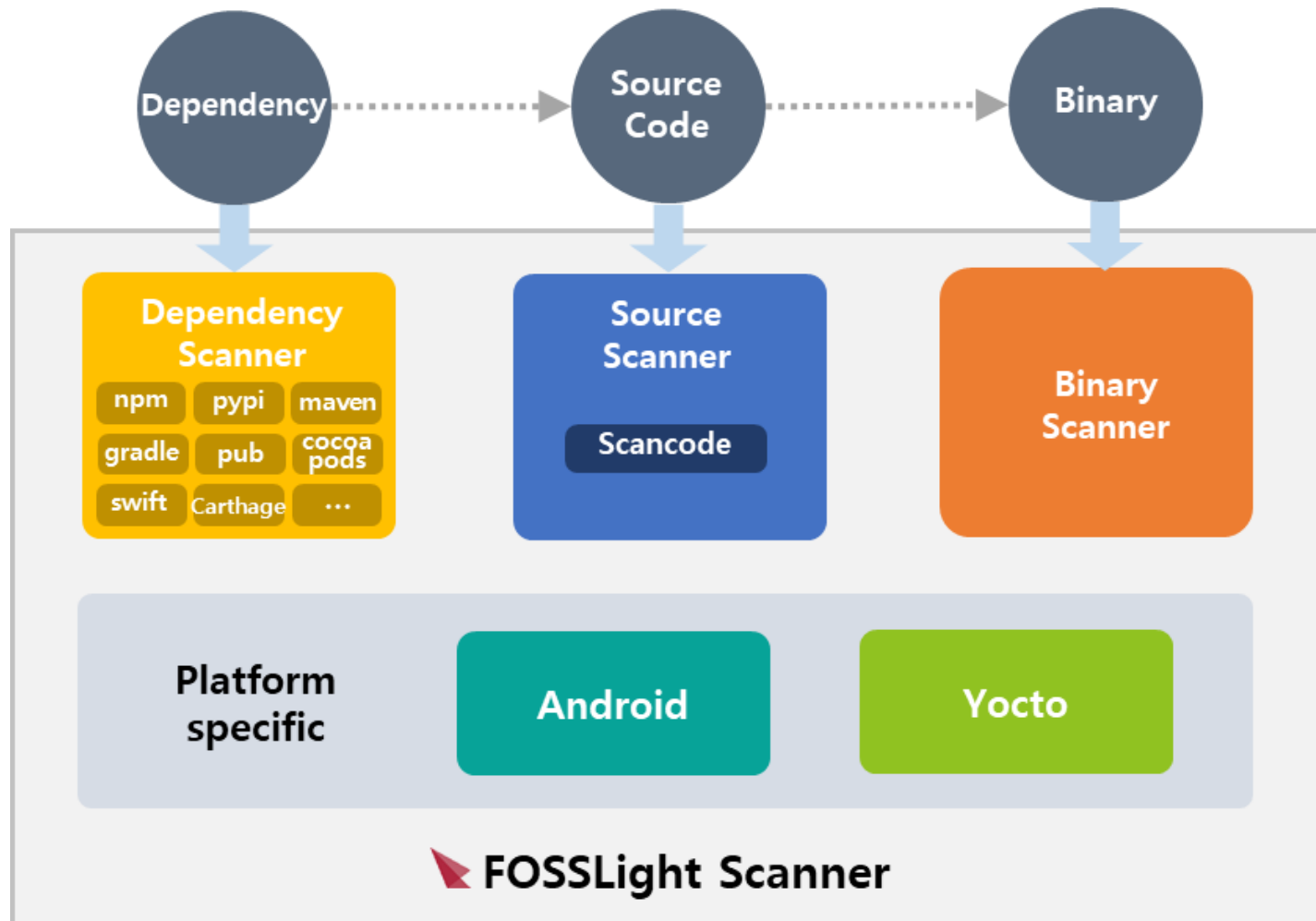
FOSSLight HUB
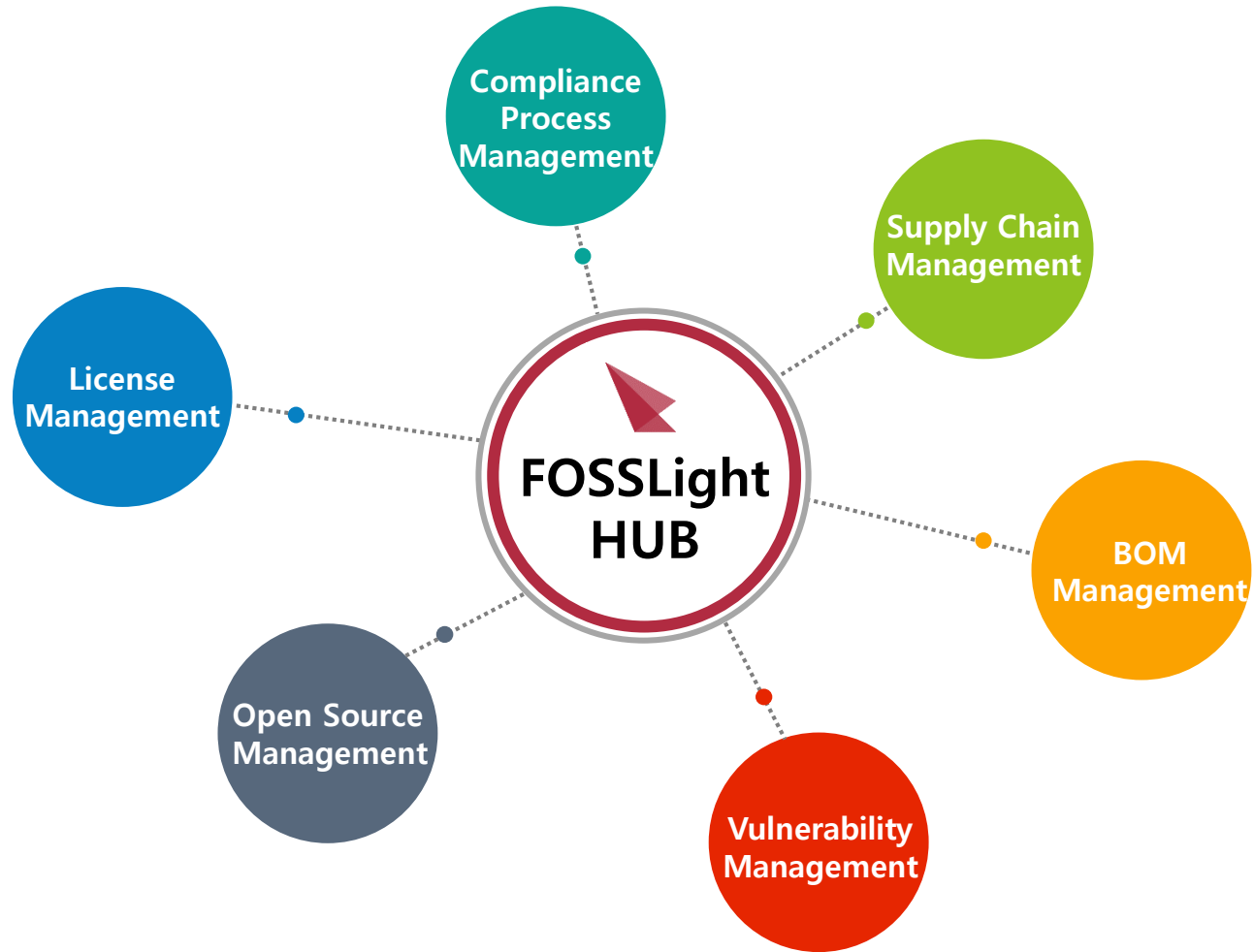
OpenChain ISO 5230

https://www.openchainproject.org
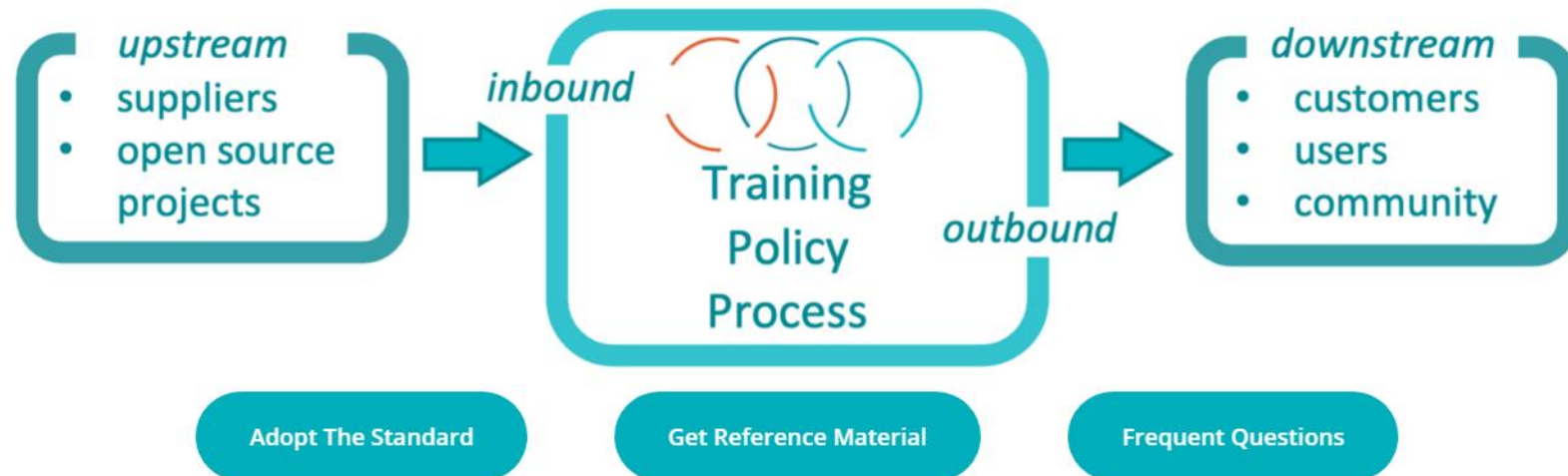
OpenChain ISO 5230 Conformance

OpenChain Spec.

1. Program Foundation
1.1. Policy
1.2. Competence
1.3. Awareness
1.4. Program scope
1.5. License Obligations

2. Relevant tasks defined and supported
2.1. Access
2.2. Effectively resourced

3. Open source content review and approval
3.1. Bill of materials
3.2. License compliance

4. Complinace artifact creation and delivery
4.1. Compliance artifacts

5. Understanding open source community engagments
5.1. Contributions

6. Adherence to the spcification requirements
6.1. Conformance
6.2. Duration

FOSSLight Hub

Open Source Management

	OSS Name			Exact Match	Copyright Text						Search

OSS Name [   ] ☐ Exact Match   Copyright Text [   ]   **Search**

License Name [   ] ☐ Exact Match   Description [   ]

Website [   ]   Deactivate ☐

Creator [▼]   Created Date [📅] ~ [📅]   Modifier [▼]   Modified Date [📅] ~ [📅]

License Type [▼]

Expand ▲

🗎 Excel download   **Add**

	ID	OSS Typ ?	OSS Name	Version	License Name	License	Obligati ?	Download Locatic	Homep	Description	Vulne bility	Creator	Created	Modifier	Modified
	23		Nick log4j	2.8.2	Apache-2.0	Permissi	🗎		URL		⚠	admin	2021-05-	admin	2021-08-
	22	D	Nick Jetty	9.4.35	Apache-2.0 OR EPL-1.0	Permissi	🗎		URL		🔺	admin	2021-05-	admin	2021-08-
+	32	V	Nick Mbed TLS	9.9.9	AGPL-3.0	Copyleft	🗎 🗎					admin	2021-06-	admin	2021-06-
	19		Nick xstream	1.4.9	BSD-3-Clause	Permissi	🗎	https://mvnreposi	URL		🔺	admin	2021-05-	admin	2021-05-
	18	M	Nick python-dateutil	2.8.1	BSD-3-Clause AND Apac	Permissi	🗎	https://pypi.org/pi	URL			admin	2021-05-	admin	2021-05-
+	16	D V	Nick JNA	5.0.0	LGPL-2.1 OR Apache-2.0	Permissi	🗎	https://mvnreposi	URL	* [Dual][V-diff] ve		admin	2021-05-	admin	2021-05-
	15	M	Nick libaddressinput		Apache-2.0 AND BSD-3-	Permissi	🗎	https://github.com	URL			admin	2021-05-	admin	2021-05-
	14		Nick QUARTZ	2.3.2	Apache-2.0	Permissi	🗎	https://mvnreposi	URL			admin	2021-05-	admin	2021-05-
	13	D	Nick node-browser-com	2.1.2	MIT OR Apache-2.0	Permissi	🗎	https://git.coolaj8	URL	Code released und		admin	2021-05-	admin	2021-05-
	12		Nick aopalliance-repack	2.6.1	EPL-2.0	Weak Cc	🗎 🗎	https://mvnreposi	URL	This Source Code		admin	2021-05-	admin	2021-05-
	11	M	Nick Gazebo	9.13.0	Apache-2.0 AND LGPL-3	Weak Cc	🗎 🗎	https://bitbucket.c	URL			admin	2021-05-	admin	2021-05-
	10		Nick Jcommon	1.0.15	LGPL-2.1	Weak Cc	🗎 🗎	https://mvnreposi	URL			admin	2021-05-	admin	2021-05-
	9		Nick mariadb-java-client	2.5.4	LGPL-2.1	Weak Cc	🗎 🗎	https://github.com	URL			admin	2021-05-	admin	2021-05-
	8	M	Nick PerconaFT	8.0.13	GPL-2.0 AND AGPL-3.0	Copyleft	🗎 🗎	https://github.com	URL			admin	2021-05-	admin	2021-05-
+	6	V	MonggoDB	4.0.4	SSPL-1.0	Copyleft	🗎 🗎					admin	2021-05-	admin	2021-05-

◁◁ ◁ Page [8] of 9 ▷ ▷▷ [15 ▼]   View 106 - 120 of 125

License Management

License Name	BSD 3-clause "New" or "Revised" License
License Type	Permissive ▾
Restriction	☐ Non-Commercial Use Only ☐ Network Redistribution ☐ Restricted Modifications ☐ Platform Deployment Restriction ☐ Prohibited Purpose ☐ Specification Constraints ☐ Restricted Redistribution ☐ Commons Clause Restriction
Obligation	☑ Notice ☐ Source Code
SPDX Short Identifier	BSD-3-Clause
Nick Name	3-clause BSD License ✕ [+ Add] BSD 3 Clause ✕ BSD 3-Clause ✕ BSD 3-Clause License ✕ BSD 3-clause New License ✕ BSD Licence 3 ✕ BSD License 3 ✕ BSD-3 Clause ✕ BSD3 ✕ BSD3_CLAUSE ✕ New BSD License ✕ Revised BSD ✕ The BSD 3-Clause License ✕ The New BSD License ✕ XML-RPC FOR C/C++ license ✕
Web site for the license	https://spdx.org/licenses/BSD-3-Clause.html
Internal URL	http://demo.fosslight.org/docx/license/BSD-3-Clause.html
	배포 시에 저작권 및 License 고지가 요구됩니다. Copyright and license notice are required when distributing the software.

Vulnerability Management

<table>
<tr><td>OSS Name</td><td>openssl</td><td>☑ Exact Match</td><td>OSS Version</td><td></td><td>CVE ID</td><td>CVE-****-****</td><td>Search</td></tr>
</table>

Export

	OSS Name	Nickname	OSS Version ⇕	Max CVSS Score
	~ [____] x	~ [____] x	~ [____] x	>= [____] x
301	openssl		0.9.8e-5	⚠
302	openssl		0.9.8e-6	⚠
303	openssl		0.9.8e-7	⚠
304	openssl		0.9.8e-8	⚠
305	openssl		0.9.8e-9	⚠
306	openssl		0.9.0b	⚠
307	openssl		0.9.0	⚠
308	openssl		0.8.3	⚠
309	openssl		0.8.2	⚠
310	openssl		0.8.1	⚠
311	openssl		0.8.0	⚠
312	openssl		0.7.17	⚠
313	openssl		0.7.16	⚠
314	openssl		0.7.15	⚠
315	openssl		0.7.14	⚠

I◄ ◄◄ | Page [21] of 26 ►► ►I [15 ▼]   View 301 - 315 of 376

Export

18

New Vulnerability Alert

[OSC] Vulnerability Discovered

« Vulnerability Information »

OSS ID	OSS Name	OSS Version	CVE ID	Score	Summary	Published Date	Modified Date
21777	mockserver		CVE-2021-32827	9.6	MockServer is open source software which enables easy mocking of any system you integrate with via HTTP or HTTPS. An attacker that can trick a victim into visiting a malicious site while running MockServer locally, will be able to run arbitrary code on the MockServer machine. With an overly broad default CORS configuration MockServer allows any site to send cross-site requests. Additionally, MockServer allows you to create dynamic expectations using Javascript or Velocity templates. Both engines may allow an attacker to execute arbitrary code on-behalf of MockServer. By combining these two issues (Overly broad CORS configuration + Script injection), an attacker could serve a malicious page so that if a developer running MockServer visits it, they will get compromised. For more details including a PoC see the referenced GHSL-2021-059.	2021-08-17	2021-08-26

* This mail was sent by osc.lge.com

Compliance Process Management

Supply Chain Management (1/2)

Search Panel:

Field		Field		Field	
ID		3rd Party Name			Search
3rd Party Software Name		3rd Party Software Version		Division	▼
Status	☐ Progress ☐ Request ☐ Review ☐ Confirm				
Created Date	☐ ~ ☐	Creator		Reviewer	

Expand ▼

Export | Add

ID ⇕	3rd Party Name	Software Name	Softwar Version	Status ?	Delivery Form	Description	Division	Creator	Created Date	Updated Date	Reviewer	Comment
410	Test 3rd party	test		C	source form		N/A	시스템관리자	2021-09-17	2021-09-17	시스템관리자	
409	Test 1234	Test		C	source form		N/A	시스템관리자	2021-09-17	2021-09-17	시스템관리자	
408	k2	k2 3rd		P	source form		N/A	K2	2021-09-11	2021-10-05	test	
407	newbie	newbie	1.0	P	source form	test	N/A	시스템관리자	2021-09-02	2021-09-07	test	
406	3rd Party Test	test1	0.1	P	source form	test	N/A	ubermen5ch	2021-08-25	2021-08-25		
405	test1	test1		C	source form		N/A	시스템관리자	2021-07-07	2021-08-03	시스템관리자	
403	test	test		R	source form		N/A	서예진	2021-06-08	2021-07-20	Vo Trung Han	
402	3rd Party Test2	3rd Party SW Name2	1.1	P	binary form	test2	N/A	hawk	2021-06-03	2021-09-01	Vo Trung Han	
401	3rd Party Test	3rd Party SW Name	1.0	P	source form	test	N/A	hawk	2021-06-03	2021-06-03	시스템관리자	
400	3rd Party Test	test	2.0	P	source form		N/A	시스템관리자	2021-05-18	2021-06-04	Vo Trung Han	
399	test software	test1	1.0	P	binary form	test software	N/A	Mike	2021-05-18	2021-05-18		

⏮ ◀ Page 1 of 1 ▶ ⏭ 15 ▾   View 1 - 11 of 11

Export | Add

Supply Chain Management (2/2)

BOM(Bill Of Materials) Management (1/2)

The National Telecommunications and Information Administration (NTIA) recently asked

Project Name	yally2 🅱 🅿		• Created	시스템관리자 (2021-06-18)

3rd party	SRC	BIN	**BOM**	↩ Reject

Show Comment History   Comment Edit ▾

Export

ID	Reference	OSS Name	OSS Version	License	Download Location	Homepage	Copyright Text	Vulnera bility	Obligation		Restriction	admin check
									Notify	Source		
	~ ☐ x	~ ☐ x	~ ☐ x	~ ☐ x	~ ☐ x	~ ☐ x	~ ☐ x	>= ☐ x				
2	SRC	CImg	2.6.7	CECILL-C	http://cimg.eu/downld	http://cimg.eu	Copyright (c) David Tschumperle (http	⚠	📄	📂	Ⓡ	☐
1	SRC	cairo	1.4.12	MPL-1.1,GPL-2.0	http://cairographics.or	https://www.ca	Copyright (c) 2002 University of South	⚠	📄	📂		☐

https://linuxfoundation.org/blog/what-is-an-sbom/

BOM(Bill Of Materials) Management (2/2)

ID		Project Name		Created Date		~			Search

Division	▼	Creator		Reviewer	

Distribution Type	▼	Network Service	▼	Model Name	

Status ☐ Progress ☐ Request ☐ Review ☐ Complete ☐ Drop

Priority ▼

OSS Name	cairo	OSS Version		License Name	

cairo
cairo123

Additional Information		Comment	

Binary Name		3rd party	

Expand ▲

☐	ID ⇕	Project Name (Version)	Status ?	Identification	Packaging	Download ?	Distribution Type	Vulnerability	Division	Creator	Created Date	Updated Date	Reviewer	Additional Information
☐	35	kkk1234 (ver v1.0)	P	Confirm 3rd SRC BIN BOM	Start	📄	General Model	⚠	N/A	희희희	2021-07-05	2021-07-05	시스템관리자	
☐	33	kkk123 (ver v1.1)	P	Confirm 3rd SRC BIN BOM	Start	📄	General Model	⚠	N/A	희희희	2021-07-02	2021-07-02	시스템관리자	
☐	32	kkk123 (ver v1.0)	R	Request 3rd SRC BIN BOM			General Model	⚠	N/A	희희희	2021-07-01	2021-07-01		
☐	31	yally3	P	Confirm 3rd SRC BIN BOM	Start	📄	General Model	⚠		시스템관리자	2021-07-01	2021-07-01	시스템관리자	
☐	25	yally2	R	Confirm 3rd SRC BIN BOM	Confirm	📄 📄 🔒	General Model	⚠		시스템관리자	2021-06-18	2021-06-18	시스템관리자	
☐	24	yally	R	Confirm 3rd SRC BIN BOM	Confirm	📄 📄 🔒	General Model	⚠		시스템관리자	2021-06-18	2021-06-18		
													Vo Trung Han 테스터	
☐	23	MyProject 0617	P	Progress 3rd SRC BIN BOM			General Model	⚠		시스템관리자	2021-06-17	2021-06-17		Project 0
☐	22	kkhtest	R	Request 3rd SRC BIN BOM			B2B	⚠	N/A	김광현	2021-06-16	2021-06-16		
☐	19	testtest0	R	Request 3rd SRC BIN BOM			General Model	⚠	N/A	서예진	2021-06-11	2021-06-11		
☐	15	test_jquery (ver 0.5)	C	Confirm 3rd SRC BIN BOM	Confirm	📄 📄 🔒	General Model	⚠	N/A	서예진	2021-06-09	2021-06-09	시스템관리자	
☐	6	test_jcc (ver 1)	P	Confirm 3rd SRC BIN BOM	Start	📄	General Model	⚠	N/A	최재창	2021-06-07	2021-06-25	시스템관리자	test

|◀ ◀◀ Page 1 of 1 ▶▶ ▶| 15 ▼   View 1 - 11 of 11

Issue Tracking
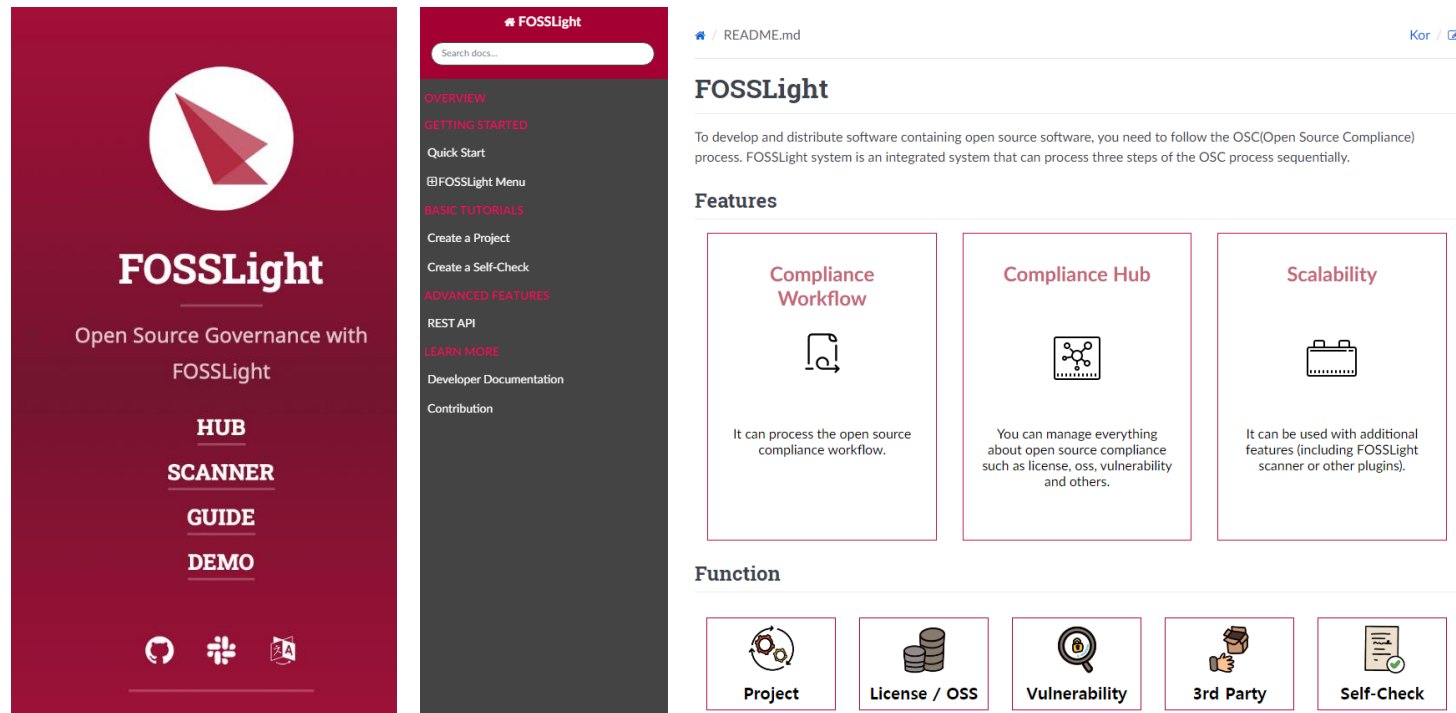
It's for communication, Please check the download location

body p

Identification > Request Review
tom.johnston | 2020-07-25 03:30:10

Identification (SRC)
tom.johnston | 2020-07-25 03:12:49

#2 I changed sax-js to licence ISC.

#6 I updated the names of three @webassembly/ packages as you suggested. The OSC system changed the names back when I uploaded them. See the attached window capture.

file:///home/tom/Pictures/Screenshot%20from%202020-07-24%2013-03-27.png

Identification (SRC)
tom.johnston | 2020-07-25 03:07:18

The following open source and license names will be changed to names registered on the system for efficient management.

Opensource Names
node-redis => node_redis
@webassemblyjs/helper-api-error => webassemblyjs
@webassemblyjs/ieee754 => webassemblyjs

Identification > Rejected
hyesung.choi | 2020-07-24 23:30:15

1. There is a typo in the OSS name. Please correct.
   1) blakeemrey-change-case > blakeembrey-change-case

2. Another OSS with the same name has been registered in the OSC system. Please change the OSS name as follows.
   1) chardet/0.7.0 → node-chardet/0.7.0
   2) mysql/2.18.1 → mysqljs-mysql/2.18.1

25

FOSSLight Links

- **https://FOSSLight.org**

- **https://github.com/FOSSLight**

- **https://demo.FOSSLight.org**

- **https://FOSSLight.org/fosslight-guide**

- **https://FOSSLight.slack.com**

Open Source Program Office Youtube Channel

❑ **https://www.youtube.com/channel/UCGCKQQvHh6pgjwHmZtKi8Hw**

FOSSLight press release

LG電子、オープンソースソフトウェア管理ツールを外部に公開

(Seoul=NSP通信) minjung kim Journalist = LG電子
ンソース（OpenSource）ソフトウェア管理道具の
（FreeandOpenSourceSoftwareLight）」を最近、外

フォースライトはソースコードが公開されており、
ロードして自由に使うことができる。

フォースライトは開発者のソフトウェアを分析し、
ンソースの使用条件や義務事項を遵守しているか
な部分を開発者に知らせるなど、オープンソース
にも役立つ。

LG電子は外部に公開するフォースライトを多くの
る。実際、韓国電子通信研究院（ETRI）はオープ
め、フォースライトを使用することにした。

LG電子CTO（最高技術責任者）のパク・イルピョ
与し、技術リーダーシップを持続的に強化してい

NSP通信 minjung kim Journalist alswjd5176@nspr
著作権者ⓒ韓国の経済ニュース通信社 NSPNEWS·NSPTV。 無断転載 - 再配布禁止。

樂金電子開放FOSSLight免費下載，擴大軟體社群市占率

2021年6月3日 · 1分鐘 (閱讀時間)

【財訊快報 / 林浩博】韓聯社報導，樂金電子(066570 KS)試圖擴大在軟體社群的市占，公司周四表示其開源軟體管理工具如今可供外部開發者使用。 樂金稱FOSSLight(Free and Open Source Software Light)系統現在可從官網免費下載。

樂金的FOSSLight這系統可檢視原始碼的合規過程。該系統可分析開發者軟體，檢驗其是否遵循授權條款與滿足安全性要求。

樂金希望此舉可擴大自家系統在全球的市占率，並透過從各式外部程序員收到的反饋改善系統穩定性。

這舉動也是樂金試圖藉由擴大合作加速數位化進程。

自2007年以來樂金就試著建立穩定的原始碼授權管理系統。

Contribution Item

Your attention, please.

Thank YOU !!