



Setting the context

Introduction: What is open source software?

Open source software (OSS) is a software programme with a source code that anyone can check, modify, and update. It is usually developed in a collaborative manner and released under a licence that allows the developer to inspect, change, and distribute the software to anyone for any purpose.

The way an organisation can use an open source software programme depends on its licence. Hundreds of different open source licences are available; each has its own terminologies and restrictions.

The two main categories of OSS licences are permissive and copyleft.



Permissive

- Allowed to use the source code for any purpose
- Attribution or acknowledgement for creators / authors is necessary
- Minimal restrictions on licence use
- Can be a part of proprietary software programmes

Examples

- Berkeley Software Distribution (BSD) licence
- Apache



Copyleft

- Allowed to use the source code for any purpose
- Attribution or acknowledgement for creators / authors is necessary
- No further restrictions can be placed on the code, distributed to the community as received
- Necessary to make an open source code for others to use it freely

Examples

- GNU General Public Licence
- Eclipse

Introduction: Current situation overview

With an increase in the use of OSS in organisations, managing and optimising OSS effectively is important. This can help organisations manage risk, compliance, and security vulnerability associated with open source components consumed internally.

Did you know?

- About **80** different types of OSS licences are available; each has its own terminologies and restrictions.
- According to Gartner, OSS is used by more than **95%** IT organisations worldwide.
- Through 2022, the **percentage of open source within IT portfolios** relative to either homegrown or licensed third-party solutions will **increase at a** compound annual growth rate (CAGR) of **30%**.

Why is it in focus now?

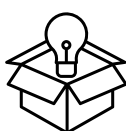
- After the COVID-19 crisis, most organisations would have remote workers who can download any software with minimal restrictions.
- More organisations are shifting to easily accessible OSS to reduce dependency on paid proprietary tools.
- However, OSS has its own set of restrictions and security issues that need monitoring.

Business need for OSS compliance

Open source software come with certain requirements, which when not followed can lead to legal, operations and security issues.



IP infringement risk: licensing obligations by using open source licence for patent provisions



Restrictions on use as proprietary licence: It can mandate the release of the source code as an OSS, and provide rights to modify and distribute at no charge.



Derivative work for copyleft licences: It needs to be licensed under the same OSS licence



Copyright notices: that are required to be included in the developed code are found in the licence text and source code files



Security risk: It indicates vulnerabilities associated with source code components.

Open source software licensing requirement/rationale

Source

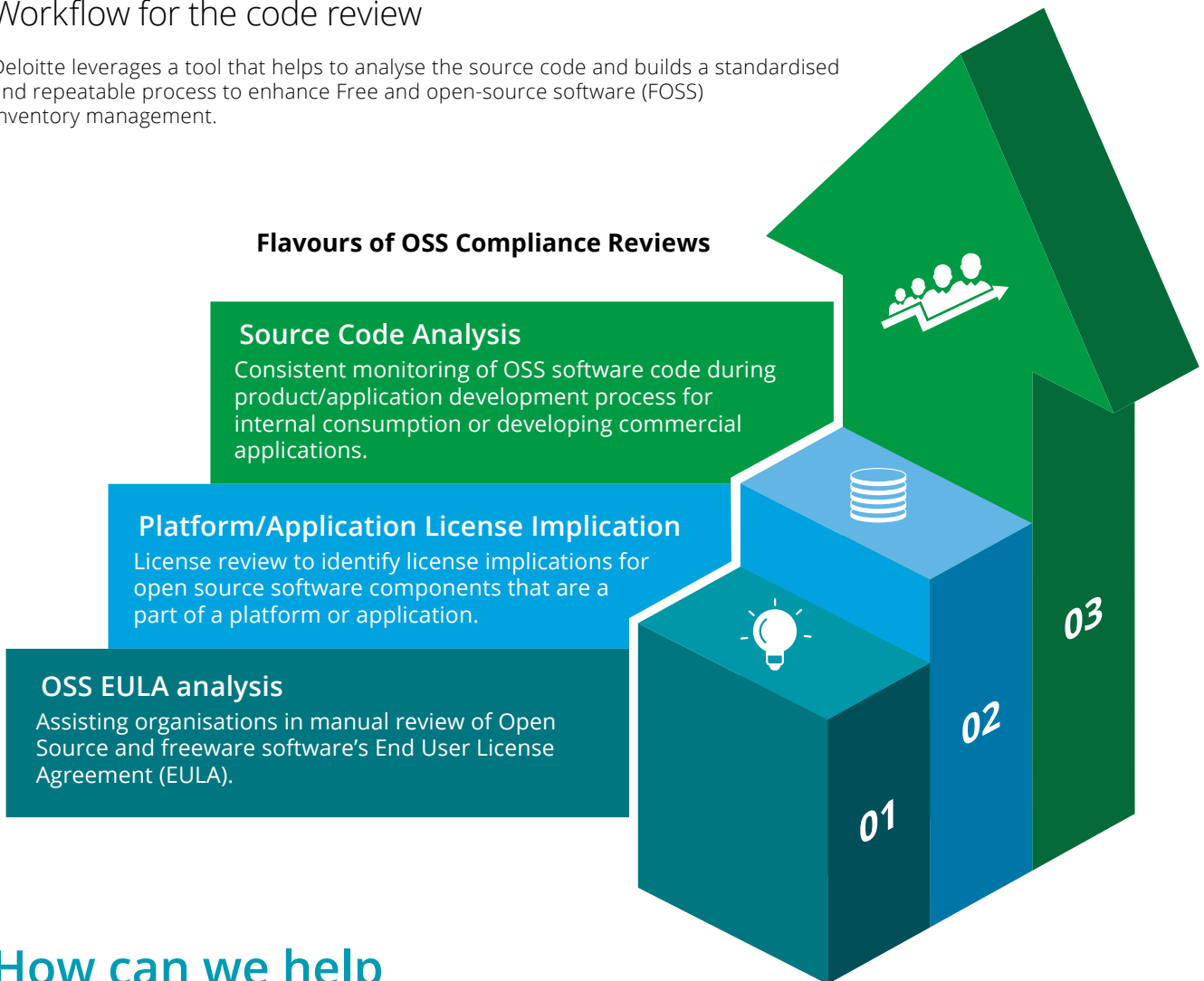
What innovation leaders must know about open-source software:
<https://www.gartner.com/document/3956651?ref=solrAll&refval=248155840>

Solution overview

Workflow for the code review

Deloitte leverages a tool that helps to analyse the source code and builds a standardised and repeatable process to enhance Free and open-source software (FOSS) inventory management.

Flavours of OSS Compliance Reviews



Source Code Analysis
Consistent monitoring of OSS software code during product/application development process for internal consumption or developing commercial applications.

Platform/Application License Implication
License review to identify license implications for open source software components that are a part of a platform or application.

OSS EULA analysis
Assisting organisations in manual review of Open Source and freeware software's End User License Agreement (EULA).

How can we help

Areas where we help organisations use OSS



Acquisitions involving OSS platform

Carry out due diligence of the application platforms and identify any potential risks posed by software licences used in building the platform.



Organisations shifting from proprietary to OSS software base

Provide consulting services on which types of OSS licences can be used in developing in-house and proprietary software.



Software applications/product development organisations

Monitor OSS software code consistently during the complete cycle of product/application development process.



OSS included as a part of the review of entire the SAM asset base

Provide a view of the OSS included in the deployment footprint and risk assessment of the installed OSS.

Contacts

Anthony Crasto

President, Risk Advisory
Deloitte India
acrasto@deloitte.com

Abhijit Katkar

Partner, Risk Advisory
Deloitte India
akatkar@deloitte.com

Kamaljit Chawla

Leader – Cyber Operate
Risk Advisory, Deloitte India
kamaljitc@deloitte.com

Tarun Kaura

Leader - Cyber Advisory
Risk Advisory, Deloitte India
tkaura@deloitte.com

Ashish Sharma

Partner, Risk Advisory
Deloitte India
sashish@deloitte.com

Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms.

This material is prepared by Deloitte Touche Tohmatsu India LLP (DTTILLP). This material (including any information contained in it) is intended to provide general information on a particular subject(s) and is not an exhaustive treatment of such subject(s) or a substitute to obtaining professional services or advice. This material may contain information sourced from publicly available information or other third party sources. DTTILLP does not independently verify any such sources and is not responsible for any loss whatsoever caused due to reliance placed on information sourced from such sources. None of DTTILLP, Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte Network") is, by means of this material, rendering any kind of investment, legal or other professional advice or services. You should seek specific advice of the relevant professional(s) for these kind of services. This material or information is not intended to be relied upon as the sole basis for any decision which may affect you or your business. Before making any decision or taking any action that might affect your personal finances or business, you should consult a qualified professional adviser.

No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person or entity by reason of access to, use of or reliance on, this material. By using this material or any information contained in it, the user accepts this entire notice and terms of use.

©2020 Deloitte Touche Tohmatsu India LLP. Member of Deloitte Touche Tohmatsu Limited