Flexera

OPEN SOURCE LICENSE COMPLIANCE

BY THE NUMBERS

Are companies under-reporting open source use?
How much are they in the dark about their potential risk?
Flexera analyzed data from 134 audit projects.

What You Don't Know Can Hurt You

Only **2%** of the issues discovered were initially disclosed **prior to audit start**

1 issue detected for every **32,873** scanned lines of code*

*Total of 1,605,496,111 lines of code scanned

367
Average # of issues found **per audit project**

Identified issues by **priority level***

P1 = 16%
P2 = 10%
P3 = 71%

Have a remediation plan in place to first manage high priority P1 issues and decrease the chance of hackers exploiting vulnerabilities.

*Priority Level Definitions

Priority Level	P1	P2	P3
Description	High severity issues such as strong Copyleft compliance issues involving the APGL and GPL, or other important vulnerabilities	Secondary priority issues related to commercial and vanity licenses	Low risk hygiene issues related to permissive licenses issues such as those under BSD, Apache, and MIT

Go Deep for Clearer, More Actionable Results

Open source use is on the rise across most industries. Collectively, using OSS saves businesses

$60 billion a year*

*Source: Entrepreneur Handbook

2x *the number of issues found in a* **Forensic Audit VS. Overview**

Flexera's Overview and Forensic Audits

WHAT IS AN OVERVIEW AUDIT?

Reports on evidence of copyright detection, license detection, exact file match to known open source content, email/URL detection, envelope issues, and binary analysis.

WHAT IS A FORENSIC ANALYSIS?

All of the detection included in Overview audits, plus extensive use of source code fingerprint analysis to identify and explain the origin, i.e. partial matches such as cut-and-paste by developers.

Compared to Baseline Audits, M&A Audits discovered

30% more **P1** issues
224% more **P2** issues
245% more **P3** issues

ONLY 37%

of companies have policies in place for **open source management**

What Companies Should Be Asking About Their Open Source Use

Goal is to always have answers to the following questions:

- *Who wrote it?*
- *Where is it deployed?*
- *Are there issues with it?*
- *Have the issues been fixed?*

DEVELOPERS
- What is being shipped?
- What open source packages are we using?
- Do we have redundant and/or outdated technologies?

LEGAL AND SECURITY
- Which applications contain known vulnerabilities?
- What are the open source disclosures for a product?
- Are we compliant with the open source license obligations?

ENGINEERING MANAGEMENT
- Where are we using open source across the company?
- What is the impact of known vulnerabilities?
- Have scheduled remediation actions been completed?

THIRD PARTIES/SUPPLY CHAIN
- What open source/commercial packages are in these binaries?
- Have known security issues been resolved?
- Is there compliance with all third-party licenses?

CONTACT US TODAY

Flexera

Speed toward enhanced OSS risk management, security and compliance using a complete end-to-end solution. Flexera offers easy-to-use tools while also reducing your remediation costs.

flexera.com