# **Open Source in M&A Transactions**



Ibrahim Haddad, Ph.D.

VP of R&D and Head of Open Source
Samsung Research America

@IbrahimAtLinux IbrahimAtLinux.com

Oskar Swirtun
Founder and CEO
FOSSID AB

Oskar.Swirtun@fossid.com

# Agenda

- Open source is inevitable
- Open source usage models
- Open source in M&As
- Source code audits
- IP audits
- Insights gained (technical, business, legal)
- Preparing for an audit (target, acquirer)
- Recommendations (target, acquirer)

Open source is inevitable.

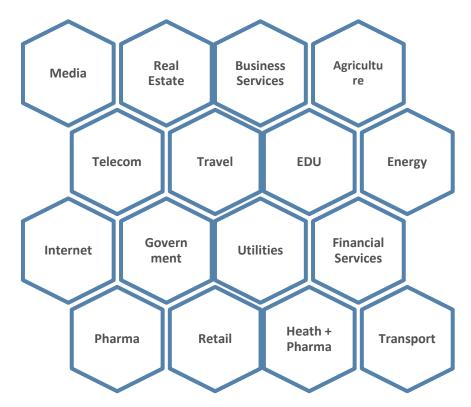
# THE WALL STREET JOURNAL.

#### **ESSAY**

# Why Software Is Eating The World



By MARC ANDREESSEN August 20, 2011

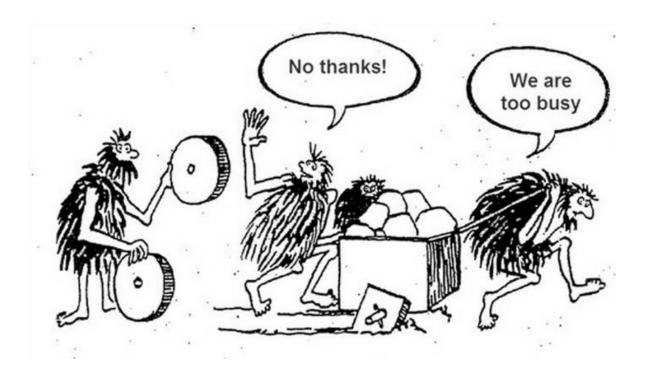


## THE WALL STREET JOURNAL.

# Open Source 'Eating' Software World: Samsung

By RACHAEL KING May 5, 2014 5:51 pm ET

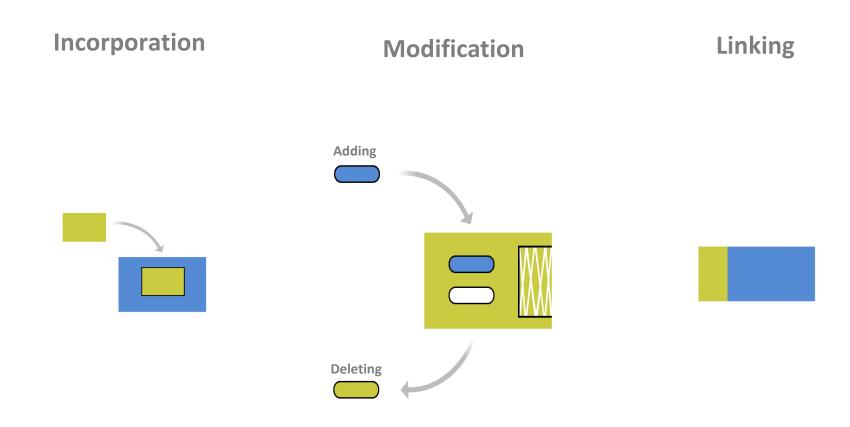
San Francisco, Calif. — Samsung Electronics Ltd. is aiming for more of a leadership role in various open source projects partially because so many of its products – from refrigerators to mobile devices—now depend on open source software.



Open source is the new normal.

Companies must master open source if the are to master software.

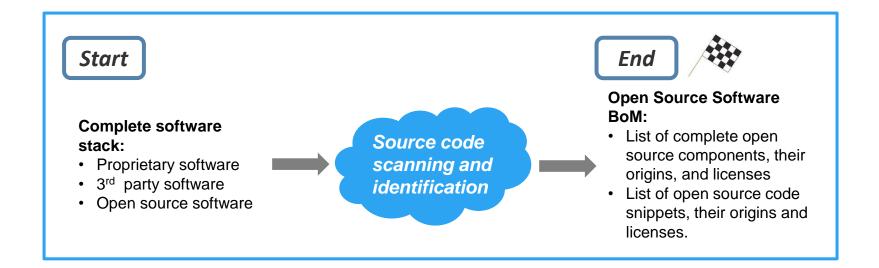
# Common open source usage scenario



**Every deal is different.** 

Open Source is a constant.

What specific due diligence open source software is required in M&A transactions?



# **Audit methods**

- 1. Traditional
- 2. Blind
- 3. Do-It-Yourself (DYI)

## **Traditional**



#### Start

#### **Initial Meeting or Call**

A call kicks off the project, introduce contact persons from all parties and communicate relevant details of the audit.



#### **Delivery of Reports**

Deliver the reports to the potential buyer, including the Bill of Materials, SPDX\* report, and an executive summary.



#### Final Meeting or Call

A call takes place to present the results of the audit and address any questions.



#### Deliver the code to auditors

Deliver the source code to the auditors via an upload to a cloud server, or invite the auditors to conduct the job on site (need to arrange for a local server to run the scans).



#### **Audit Execution**

The auditors will run the scan on the code base. They will identify the origin and licenses of open source components, and open source snippets\* found in non-open source components.



\* Not all auditors have these capabilities. Check with your audit service provider.



#### Start

#### **Initial Meeting or Call**

A call kicks off the project, introduce contact persons from all parties and communicate relevant details of the audit.



#### **Fingerprint Collector Tool**

The Command Line Interface is sent to the target company with installation and execution instructions to collect digital signatures\* of their software.



#### **Blind Audit**

FOSSID AB engineers audit the target software without having access to the source code and using only the digital signatures.



#### **Knowledge Base Comparison**

FOSSID AB will use the collection of digital signature to search their open source database looking for matches to open source files and snippets.



#### **Secure Transfer**

The collection of digital signatures is transferred securely over SSH to a dedicated server in FOSSID's datacenter.



#### **Approval Request**

Once the audit is completed, reports are sent to the target company for review before they are shared with the potential acquirer.



#### **Delivery of Reports**

After the review with target company, final reports are delivered to the potential buyer, including the Bill of Materials, SPDX, and the executive summary.



#### Final call

A final call takes place to present the audit results to the potential buyer and address any questions.











#### Start

#### **Initial Meeting or Call**

A call kicks off the project, introduce contact persons from all parties and communicate relevant details of the audit.

#### **Fingerprint Collector Tool**

The Command Line Interface is sent to the target company with installation and execution instructions to collect digital signatures\* of their software.







#### **Upload & Scan**

The target company uploads the digital signatures to the WebApp and runs the scan.

#### **Online Initial Setup**

FOSSID AB runs an initial session with the target company explaining how to operate the tool (run scans, review results, generate reports).

#### **Dedicated WebApp**

FOSSID AB provides the target company with time limited access to a dedicated instance of their Web Application.









#### End

#### **Audits Your Own Software**

The target company can now audit their code, inspect all file and snippet matches to FOSSID's open source database, and generate a Bill of Materials and SPDX conformant reports.

#### **Independent Verification**

FOSSID AB compliance engineers randomly verifies the audit results of 1% of the files set forth to be audited.

#### Audit End & Data Deletion

Once the DIY Audit time limit is reached. the WebApp instance and all related information is wiped out from FOSSID's systems and an official confirmation of deletion is sent to the target company.

# Sample reports







### **Bill of Materials PDF**

Basic Bill of Materials or software inventory categorized by component that includes all identified files and the corresponding metadata.

## **Portable Dynamic Report**

Interactive self-contained HTML report that provides advance features to filter and investigate the report results. It works offline.

## **SPDX Conformant Report**

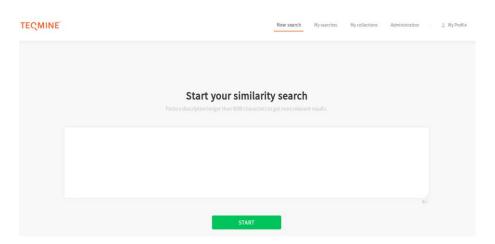
Software Package Data Exchange (SPDX) conformant XML file that serves as software inventory that can be imported into other compliance tools.



# IP Audits Extended M&A Due Diligence

# **IP Audit – Teqmine**

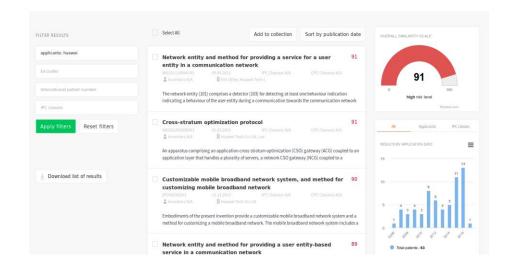
Describe your idea or copy-paste a a full patent text or a full text product or invention description



Compare to millions of full-text patents

Visualize, explore or technology automate monitoring

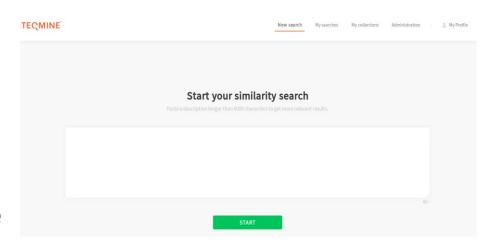
Analyze 12M+ patents in seconds



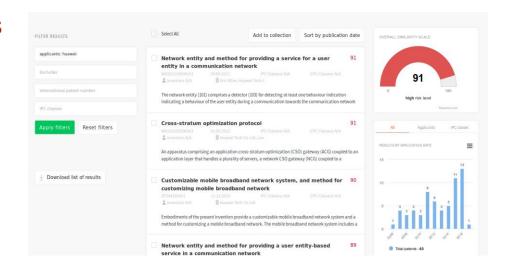
## **IP Audit – Teqmine**

Ensure freedom to operate in the new area before you enter and understand Intellectual Property landscape for products based on the acquired technology

Technology Map illustrates the position of the products, inventions or patents, and puts these in the context of existing patents



Analyze 12m+ patents in seconds



**Demo of IP Audits – Teqmine** 

What insights can you learn from such preacquisition compliance diligence?

# **Engineering**

- 1. Modularity of software components.
- 2. Integration of various components or modules.
- 3. Transparent APIs.
- 4. Documentation.
- **5.** Source code organization including the separation of open source and proprietary components.

## Observations:

- Good programming practices are also legal best practices.
- High correlation between good compliance practices and good engineering practices.

# **Legal and Compliance**

1. Receive insights on policies and processes setup to handle open source compliance at target company.

Including adequate mechanisms to satisfy open source license obligations.

2. Learn about open source development practices that may conflict with the acquiring company's open source policies:

To what extent, and a way to compare the target company's record of fulfilling of open source license obligations for current commercial offerings.

- **3.** Discover proprietary software assets are at risk due to misuse of open source software with strong copyleft license.
- **4.** Understand the compliance risk portfolio of the target company:

The open source licenses the target uses and if it is aligned with the comfort zone of the acquiring company.

- 1. A better understanding of whether the bulk of the target's valuation is a result of the integration of open source or in proprietary added value.
- 2. A confirmation whether the target company has identified all open source software contained in distributed products and services and whether or not they've satisfied all obligations resulting from mixing the open source code with code under a proprietary or alternative open source license.

**Preparing for an audit** 

Process and policy

Staff

**Training** 

Tooling

Measure up your compliance efforts

# **Preparation – Avoid common pitfalls**

Туре	Avoidance
Unplanned inclusion of copyleft FOSS into proprietary or 3 <sup>rd</sup> party code (or vice versa).	Training. Regularly scheduled scans.
Unplanned linking of FOSS into proprietary source code (or vice versa).	Training. Dependency tracking tool.
Failure to provide accompanying source code.	Checklist. Post shipping to-do.
Providing the incorrect version of accompanying source code.	Update process to ensure that the accompanying source code for the binary version is being published.
Failure to provide accompanying source code for FOSS component modifications.	Update process to ensure that source code for modifications are published.
Failure to mark FOSS source code modifications.	Training. Verification before posting source code.
Failure by developers to seek approval to use FOSS.	Conduct periodic full scan to detect undeclared FOSS. Training. Accountability (including compliance in performance metrics).
Failure to audit the source code.	Provide proper staffing. Enforce periodic audits.
Failure to resolve the audit findings.	Time limit before escalation kicks off automatically.
Failure to seek review of FOSS in a timely manner.	Training.

# **Preparations**

Choose the right audit model and right auditor for your needs

Know what you care about

Ask the right questions

Identify items to be resolved before executing the transaction

Create a compliance improvement plan for post-acquisition

# Recommendations

Identify the origin and license of all internal and external software.

Track open source software within the development process (components and snippets).

Perform source code reviews for all code entering your build system or repos.

Fulfill license obligations when a product ships or when software is updated.

Offer open source compliance training to employees.

Decide with the target company on the appropriate audit method to use, and which 3rd party to engage for the audit

- o Audit method, inputs and outputs
- o Primary contact
- o Timeline and logistics especially if it involves an on-site visit
- o Confidentiality parameters
- o Code vulnerabilities and version control (which method is your provider using)

**Summary** 

## **Final Thoughts**

Open source compliance is an ongoing process, not a destination.

Ensuring compliance is a practice that must ne maintained regardless of any potential corporate transaction.

Maintaining good open source compliance practices enables companies to be prepared for any scenario where software changes hands, from a possible acquisition, a sale, or product or service release.

New paper coming soon.

# **Open Source in M&A Transactions**



Ibrahim Haddad, Ph.D.

VP of R&D and Head of Open Source
Samsung Research America

@IbrahimAtLinux IbrahimAtLinux.com

Oskar Swirtun
Founder and CEO
FOSSID AB

Oskar.Swirtun@fossid.com