Software Audit for Acquisition Due Diligence

What to expect as a Seller

Agenda

- About nexB
- Software Audit for Acquisitions
  - Software Audit Scope
  - Software Analysis Deliverables
  - Software Audit Process with details
  - Software Audit Tools
- Why nexB

About nexB

- OSS license compliance applications and tools
- Software provenance analysis services

- Software audit services

Acquisitions

Software product lifecycle compliance

Expertise in all languages and platforms

- Active **OSS developers**
  - **ScanCode Toolkit**
  - **ScanCode Workbench**
  - **AboutCode Toolkit**
  - **and many other projects**

THE LINUX FOUNDATION

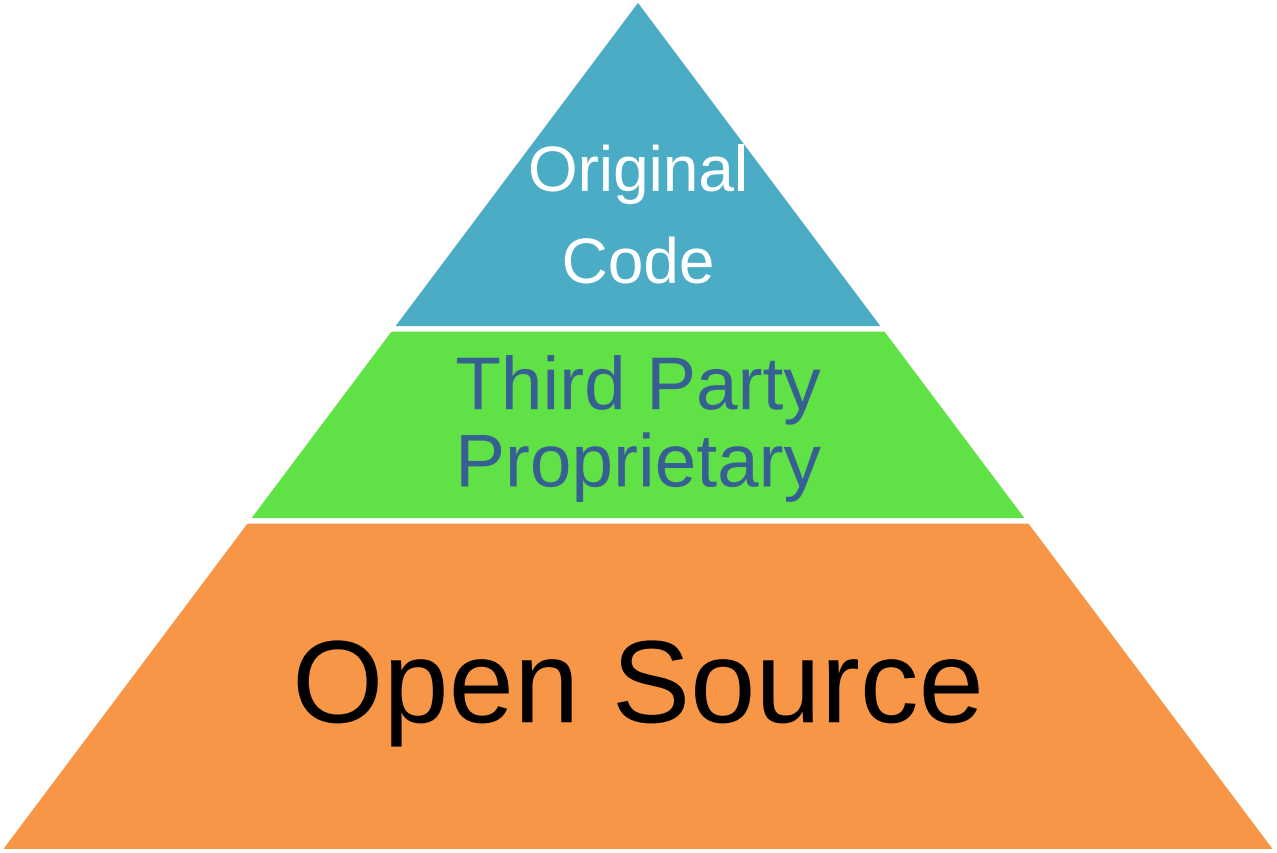
nexB

Software Audit Overview

- Identify potential software license risks for Buyer
  - Open source software
  - Commercial and other third-party software
  - Original Seller code

- Need trusted third party like nexB
  - Mitigates confidentiality concerns of a Seller company
  - Maintains segregation of information during acquisition negotiations
  - Enables objective analysis of issues with appropriate consideration of feedback from all parties

Software Audit Scope



Modern software products comprise 70% or more open source
or other third-party components

Software Audit Deliverables

- Complete inventory of OSS and third-party components in Development codebase(s)
- Bill of materials for each Product (as Distributed or as Deployed on Cloud or a device)
- Specific list of Issues and recommended remediation Actions
  - Primary focus on Copyleft- and Commercial-licensed code
  - Detailed analysis for Copyleft “contamination” as needed
  - Checklist of commercial components provide a cross-check for parallel review of software supplier contracts

Software Audit Process

Schedule Parameters

- Preparation – up to 1 week
- Analysis – 1 to 3 weeks depending on audit scope and size of codebase(s) under audit
- Draft Report – 1 day to 1 week
- Final Report – 1 day to 1 week

1: Preparation

- Establish NDA between nexB and your company
  - Two-way (nexB/Seller) is easiest
  - nexB will already have complementary NDA with Buyer
  - Three-way (nexB/Seller/Buyer) is possible
- Understand our Software Audit Process
  - One hour or less conference call to go through the audit steps with you and your team

➔ You may be anxious about the process:

- We help you understand our process to make you comfortable
- Our NDA terms ensure that you see our findings and report before the Buyer does

1: Preparation

- To scope the audit effort, we need
  - Background information about the product(s) and codebase(s)
  - Initial scans of the codebases (with nexB ScanCode tool)
  - Disclosure of known third-party and open source software
  - Platform, installation and other relevant documentation

➔ We try to minimize the impact on you

  - Except for the scans we are only asking for information that you already have at-hand
  - The disclosures you provide are important, but we do not ask you to create any special documentation for the audit

2: Analysis

- After nexB has access to the code, we schedule a telephone interview:
  - One hour or less
  - Involved your senior technical contact(s)
  - Goal is to understand your development process and open source and third party policies in greater details

➔ We limit our demands on your team because we know you are already over-tasked during acquisition due diligence.

  - We may need quick (24 hour) responses to some technical questions
  - We will usually need quick review of our findings

2: Analysis

Analysis Activities:

- Scan files for license and copyright texts
- Match target code to reference code repository for origin and license detection (based on digital “fingerprints”)
- Map Deployment code to Development code to:
  - Validate that we have all of the Deployed code
  - Identify packages provisioned from a repo (Maven etc.)
  - Identify actual open source and other license obligations – most open source obligations apply only to components that are deployed or distributed
- Analyze software interaction and dependency patterns for Copyleft-licensed components
- Investigate commercial licenses as much as possible from public sources

2: Analysis

Analysis Results:

- Software Inventory for Development Codebase
- Bill of Materials for each Distributed or Deployed Product
- Draft Issues-Actions

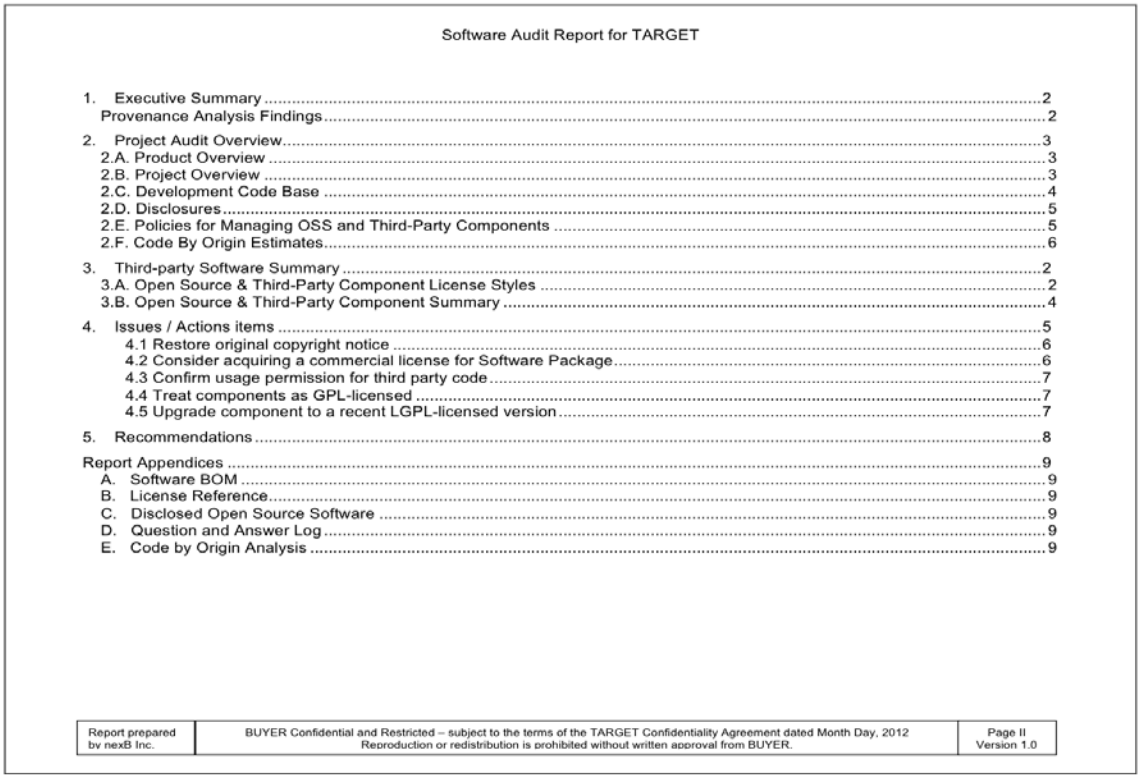
BOM Ref #	Location	Component	Version	Origin	License Style	License	Match Level	Code Type	Attribution	Redistribution	Patent Impact	Modified	Deployed	Interaction	Action	Notes	URL to Original code	Location of License Text
1000	/xxx/xxx/xx.xxx	xx.xxx	v1.6R3	Mozilla Rhino	Copyleft	Choice of NPL 1.1 or GPL 2.0 (future versions under Choice of MPL 1.1 or GPL 2.0)	Library	Binary	x	x	x		Y		Upgrade to version 1.7R1 or higher, or make sure the offending debugger binaries (which are not used in the product code base) are removed from the redistributed 1.63R Rhino jars. Rhino 1.7R1 or higher DOES NOT have proprietary Sun code in it.	There are license issues with all versions prior to version 1.7R1 leading Mozilla to remove the debugger code from the component distribution in recent releases. The debugger contains non-open source SUN proprietary binaries in: js.jar/org/mozilla/javascript/tools/debugger/downloaded/ The license prohibits modification and redistribution.	http://www.mozilla.org/rhino/	http://developer.mozilla.org/en/Rhino_License
1020	/xxxxxx/xxxx/xxxx/xx/xxx/xxx/ XXXXXXX/xxx/xxxxxxx/xxxxxxx xxxxxxx.xxxx	xxxxxxxxxxxxxx .xxxx		SwingPix Photo Organizer	Copyleft	GPL 2.0	File	Source	x	x	x		Y		Replace or rewrite to avoid GPL impact	Match with swtemary.c file from swingpix. This file is included in a standalone tool otherwise already GPL-licensed. The original notice has been removed.	http://sourceforge.net/projects/swingpix/	
1090	/xxxxxx/xxxx/xxxx/xxx/xxx/xxx x/xxxx/xxxxYY.xxxx	xxxxYY.xxxx		Oracle/Sun Java JDK	Commercial	Sun Binary Code License Agreement	Snippet	Source				x	Y		Replace or rewrite or obtain commercial license from Oracle. Alternative implementations are available under non-copyleft licenses such as in Apache Harmony.	Match with JDK's java.util.prefs.Base64.java file . The JDK license does not grant rights to modify and redistribute JDK code in source or binary form	http://www.oracle.com/	
1120	/xxxxxx/xxxx-xxxxxx-xxx/xx/xxxxxxxx/xxxxxxxxx/	xxxxxxxxxxxxx xxxxxxx.xxxx		MySwing	Copyleft Limited	LGPL 2.0	Snippet	Source	x	x	x		Y	Static linking with LGPL	**Replace or rewrite to avoid LGPL impact**	120 lines match starting at line 12 with EventHandler.java from MySwing. This snippet makes the files and all the proprietary code depending on this or built in the same Jar potentially subject to the LGPL.	https://myswing.dev.java.net/	Source file header
1130	/xxxxxx/xxxx-xxxxxx/xxxxY	xxxxxY, xxxxxY	v0.97 or earlier	GNU GRUB	Copyleft	GPL 2.0	Library	Binary	x	x	x		Y			GRUB is a bootloader and does not interact with proprietary software.	ftp://alpha.gnu.org/gnu/grub/	
1150	/xxxxx/xxxx_xx/xxxx/xxxx/xxx/ xxxx/xxxxxxx/	xxxx_xxxx.x		NetBSD	Attribution	BSD-Original	Snippet	Source	x			x	Y		**Replace or rewrite or demonstrate compliance with BSD Original license**	75 lines match starting at line 23 with print-ascii.c from NetBSD. The BSD Original license has extensive advertising obligations.	http://www.netbsd.org/	
1160	/xxxxx/xxxx_xx/xxxx/xxxx/xxx/ xxxx/xxxxxxx/	xxxx_xxxx.x		Libcddb	Copyleft Limited	LGPL 2.1	Snippet	Source	x	x	x	x	Y	Static Linking with modified LGPL	**Replace or rewrite to avoid LGPL impact**	70 lines match starting at line 56 with cddb_net.c, LGPL-licensed.	http://libcddb.sourceforge.net/	
1170	/xxxxxx/xxxx-xxxxxxx-xxx/xx/xxxxxxx/xxxxxxxx/xx x/xxxxxx/xxxxxxxxxxx/xxxxxxx xxx/	xxxxxxx.xxxx		LizardWorks TIFF Library	Copyleft	GPL 2.0	Snippet	Source	x	x	x		Y	Linking with GPL	**Replace or rewrite to avoid GPL impact**	54 lines match starting at line 200 with IDFEntry.java from the Lizardworks TIFF library.	http://www.lizardworks.com/libs.html	Copyleft.txt in original source archive
1180	/xxxx/xxxxxxx/xxxxx/xxx/xx/xx xx/xxxxx/xxxxxxxxxx.xxxx	xxxxxxxxxx.xxx x		Scientific Annotation Middleware	Attribution	Apache 1.1	Snippet	Source	x			x	Y		**Restore original license notice**	89 lines matchy starting at line 345 with file ExitStatus.java. Original Apache 1.1 software license notice missing	http://sourceforge.net/projects/sam/	
1210	/xxxx/xxxxxxx/xxxxx/xxx/xx/xx xx/xxxxx/xxx/xxxxxx/xxx-/xxxxxxxxxxxxxxxx-.xxxx	xxxxxxxxxxxxx xxxxx-.xxxx		Atlassian spring-portlet-sample	Attribution	Apache 2.0	Snippet	Source	x		x	x	Y			30 line match with file named "Uploadlib-.java" under "/spring-portlet-sample-src.zip\spring-portlet-sample\xxxx-INF\src\org\springframework\xxxx\portlet\sample"	http://opensource.atlassian.com/confluence/spring/download/attachments/10/spring-portlet-sample-src.zip	
1230	/xxxxxx/xxxx/xxxx/xxx/xxxxx-xxxY.Y/	xxxxx-xxxY.Y	vcvs-20060406	JRadius	Copyleft Limited	LGPL 2.1	Library	Binary	x	x	x		Y			LGPL 2.1 for the core development kit, GPL 2.0 for the applications. Only the development kit is used.	http://downloads.sourceforge.net/jradius/jradius-cvs-20060406-java15.zip	http://jradius.sf.net/license.html and License file in the original distribution
1240	/xxxx/xx/xxxxxxx/xxxxxxx/xxxx xxx/xxx/xxx/xxxxxx/xxxxxxxx xxxx.xxxx	xxxxxxxxxxxx. xxxx	v1.5.0-06	Oracle/Sun Java JDK	Proprietary	Sun Binary Code License Agreement	Snippet	Source	x			x	Y		**Replace or rewrite or acquire commercial license from Oracle.**	57 lines match starting at line 45 with Arrays.java from the JDK. The JDK license does not grant rights to modify and redistribute JDK code in source or binary form.	http://java.sun.com/javase/index.jsp	
1310	/xxxx/xx/xxxxxxx/xxx/xxxxxx/x xxxxxxxxxxx.xxxx	xxxxxxxxxxx.x xxx		JRobot	Attribution	BSD-Modified	Directory	Source	x			x	Y		**Restore original license notice**	License/notices from the origin are missing in the source files.	http://sourceforge.net/projects/jrobot/	
1360	/xxxx/xx/xxxxxx/xxxxxxx/xxxx xxx/xxxxxxxxxxxxxxxxx.xxxx	xxxxxxxxxxxxx xxxx.xxxx		Blitz JavaSpaces	Attribution	BSD-Modified	File	Source	x			x	Y				http://sourceforge.net/projects/blitzjavaspaces/	

3: Draft Report

- Issue-Action List
  - Specific and actionable actions to remediate or mitigate
  - Review draft with product team: *we get your review of the draft report documents before we share them with the buyer*
  - Incorporate your feedback and answers
- Report
  - Executive Summary
  - Project, product and codebase overview
  - Inventory / BOM statistics
  - Recommendations
  - Appendices
    - License Reference
    - Project documents (QA Log, Disclosures, etc.)

4: Final Report

- Final Software Inventory / BOM spreadsheets
- Final Issue-Action List (with Responses)
- Final Report Package



Software Audit Report for TARGET

Software Audit Tools

- nexB uses a combination of automated tools and review by our analysts
  - Most of our tools are already open source – see https://github.com/nexB
  - Some are nexB proprietary (will be released as OSS in future)
- Multiple layers of analysis
  - Direct scan for license and copyright notices
  - Component matching for open source and publicly available third-party components (freeware/proprietary)
  - Analysis of source code and pre-built libraries
  - Interaction and dependency analysis as needed
- Two levels of internal review by nexB experts

Why nexB

- Balanced approach
  - Automated code analysis AND analysis by software provenance experts
  - Direct consultation with engineering, management and legal teams
- Concrete Action items with
  - nexB recommended options for resolution
  - Option for Seller to share Action responses to share with Buyer
- Recognized experts in software origin analysis
- 500+ software audit projects completed to-date

Why nexB – Quotes from our customers

What they're saying.

"I will most definitely be remembering nexB, as I was very impressed by your scan and how smooth the process was."

"Again, thank you for all the work you and your team did. It was exactly what we needed."

"It was our pleasure to work with you and your team. nexB was really professional and had an impressive analysis."