

 **BLACKDUCK**

 **ManageWare**
THINK Beyond

Black Duck Seamless ALM Integration

How to integrate Open Source
Governance as part of your
Application Lifecycle Management

Aviram Ganor – Manageware

 **BLACKDUCK**

 **ManageWare**
THINK Beyond





“

Open source is a ‘silver bullet’ that allows simultaneous improvement along all three dimensions of the software ‘iron triangle’ of cost, schedule, features.

”



“

Open source is ubiquitous, it’s unavoidable....having a policy against open source is impractical and places you at a **competitive disadvantage**.

”



BLACKDUCK

ManageWare
THINK Beyond

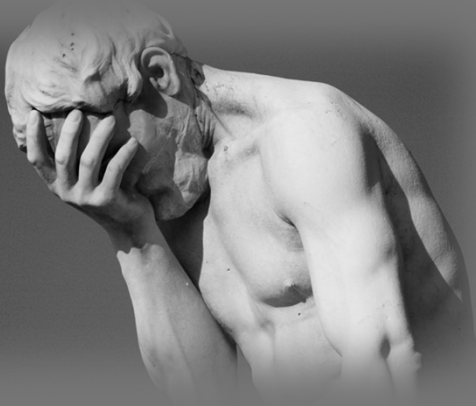
FOSS is not a free lunch...



BLACKDUCK

ManageWare
THINK Beyond

So what can go wrong?



 **BLACKDUCK** 

FOSS Management & Governance

Strategy


Policy & Process


Technology


 **BLACKDUCK** 

Strategy

- Articulation of the business goals
- Enables the transition from defensive/reactive to offensive/pro-active use of FOSS
- Strategy addresses at a business level
 - Where FOSS will be used
 - In order to accomplish what objectives
 - How these objectives will be achieved



 **BLACKDUCK**



Policy and Process

- **Policy**
 - The rules for evaluating, approving, using and releasing FOSS code
 - Created & managed by key stakeholders
- **Process**

The way policy is reliably realized on a day-to-day basis
Interwoven with existing development and product release processes:

 - Acquisition & Approval
 - Component Update
 - Release
 - Compliance

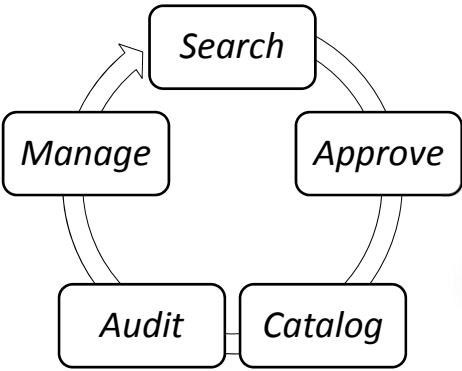


 **BLACKDUCK**



Technology

Black DuckTM Suite






Centralized Searching



Centralized Search Console

- OSS/3rd party Components
- Approvals/Requests
- Licenses
- Sec Vulnerabilities

Simple Search Results

Used By All Roles In The Organization






Internal Code Search for Reuse

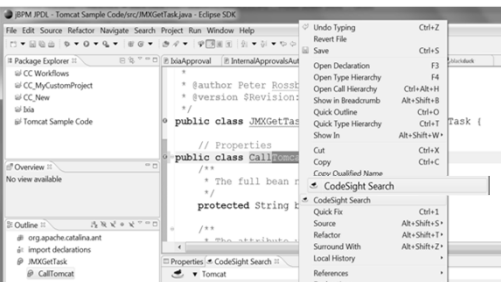


Enterprise Search

- 35 Languages
- Eclipse & Visual Studio Plug-Ins

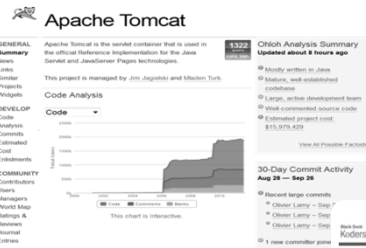
Index and Search Internal Code

- Version Controls Integrations
 - ClearCase
 - CVS
 - Git
 - Mercurial
 - Perforce
 - Subversion
 - Team Foundation Server
 - Visual SourceSafe
 - Flat File Systems
 - Zip, Archive






Free OSS Web Resources



Apache Tomcat

Ohloh Analysis Summary
Updated about 8 hours ago

Code Analysis

30-Day Commit Activity
Aug 28 -- Sep 26

<http://www.ohloh.net>

Free OSS Directory Linking
People and Projects

- Development Analysis
- Rankings And Comparisons
- Contributor Profiles

<http://www.koders.com>

Free Code Search

- Over 3.3. Billion Lines Of Code
- 35 languages
- Eclipse, Visual Studio, Browser Plug-Ins






Create Component Request

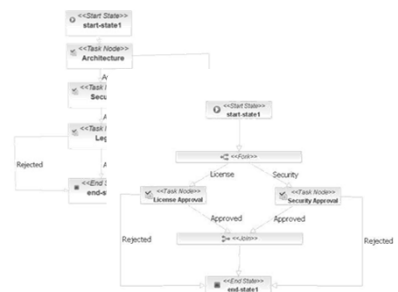


Create Request

- Search OSS Components
- Search Pre-Approved Catalog
- Begin The Request Process

Configurable Approval Workflow

- Approval Path
- Approval Boards
- Request Wizard
- Global or Project Based



```

graph TD
    Start([start-state1]) --> Arch[Architecture]
    Arch --> Sec[Security]
    Sec --> Lic[License]
    Lic --> App[Approved]
    App --> End([end-state1])
    Arch --> Rej1[Rejected]
    Sec --> Rej2[Rejected]
    Lic --> Rej3[Rejected]
    
```




Complete The Request Form

Create Requests

Select Components > **Select Applications** > Select Approvers > Select Developers > Complete Request Form

Select application and click "Add To Request"

Search: Go

2 items (10 per page) Columns...

Application	Version	Description	Workflow Name
External Retail Project	2.1		Simple Flow
My Application Project	V1.5		Internal Auto Approval

Add To Request

Customizable Request Form

- Important Questions
- Provide Additional Info
- Reviewed By Approvers

Wizard Steps Through The Request Process

Select Components > Select Applications > Select Approvers > Select Developers > **Complete Request Form**

Complete the request form for each component and either save or submit your requests

View Component Details

Application: External Retail Project - 2.1

Licenses: Apache License Version 2.0

Usage: Component (Dynamic Library)

Request New Component Form

Describe the functionality provided by this component and the problem it solves. Application Server

What alternative components have you considered?

How will the component be distributed? Customer Facing

Has the component been checked into source control? ☐ Yes ☒ No




Review Request Details



Email Notification Of Component Request

Review Request Details

Approve Or Reject The Request

Request Form Approvals Component Details Vulnerabilities(0/31) Developers More...

Creation Date: September 26, 2011

Submission Date: September 26, 2011

Request Status: Pending

Additional Component Request Information

Request New Component Form

Describe the functionality provided by this component and the problem it solves. Application Server

What alternative components have you considered?

How will the component be distributed? Customer Facing

Has the component been checked into source control? ☐ Yes ☒ No

Request Form Approvals Component Details Vulnerabilities(0/0) Developers More...

Approval Sends Request To Next Board/Person In Workflow




Review Security Vulnerabilities

Request Form

Approvals

Component Details

Vulnerabilities(0/31)

31 Vulnerabilities (1 - 10) 10 per page Columns... Jump...[First]< Prev[Next]>[Last]

Name	Severity	Date	Description	Comments	Review Status
CVE-2011-3190	High	August 31, 2011	Certain AJP protocol connector implementations in Apache Tomcat 7.0.0 through 7.0.20, 6.0.0 through 6.0.33, 5.5.0 through 5.5.33, and possibly other versions allow remote attackers to spoof AJP requests, bypass authentication, and obtain sensitive information by causing the connector to interpret a request body as a new request.		
CVE-2011-2526	Medium	July 14, 2011	Apache Tomcat 5.5.x before 5.5.3 6.x before 6.0.33, and 7.x before 7.0.19, when sendfile is enabled for the HTTP AJP or HTTP NIO connector, does not validate certain request attributes, which allows users to bypass intended file access restrictions or cause a denial of service (infinite loop or JVM crash).		

Tied To National Vulnerability Database

- Updated Daily
- Tracks Past Versions
- Email Notifications

Request Form

Approvals

Component Details

Vulnerabilities(0/0)

Developers

More...

Approve
Reject
Start Discussion...
Send Back To Requester...
Change Approver...




Review License Details

Request Form

Approvals

Component Details

Vulnerabilities(0/31)

Developers

More...

Name: Apache Tomcat
Version: 6.0.5
License: Apache License Version 2.0 (view)
Description: Apache Tomcat is the servlet container that is used in the official Reference Implementation for the Java Servlet Pages specifications are developed by Sun under the Java Community Process. Apache Tomcat is intended to be a collaboration of the best-of-its-kind open development project. To learn more about getting involved, click here. Apache Tomcat powers a range of industries and organizations. Some of these users and their stories are listed on the Powered by Apache page.
Release Date: July 05, 2011 12:00:00 AM
Homepage: http://tomcat.apache.org/tomcat/index.html
Programming Language: Java
Number of Contributors: 0

Apache License Version 2.0, January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

Request Form

Approvals

Component Details

Vulnerabilities(0/0)

Developers

More...

Approve
Reject
Start Discussion...
Send Back To Requester...
Change Approver...




License Obligations

Obligations:

Fulfilled	Obligation	Type
☐	You are not entitled to impose a fee related to what Recipient may do with the code.	Legal
☐	You are not entitled to place additional restrictions on what Recipient may do with the code.	Legal
☐	You are required to disclaim warranties on behalf of others.	Legal
☐	You are required to distribute the source code of the Dynamic Library.	Legal
☐	You are required to ensure that the software displays a particular notice at runtime.	Legal
☐	You are required to grant the right to reverse engineer the Dynamic Library.	Legal
☐	You are required to include a copy of the license in distributions that you make.	Legal
☐	You are required to license the entire Dynamic Library under the same terms as the original code.	Legal

Easily Review Every Licenses Obligations




License Conflict(Bill Of Materials)

Bill of Materials

License Conflict	Component Type	Component	Version	License	Usage	Ship Status
⚠	⊙	Apache Jakarta Commons FileUpload	1.1	Apache License Version 2.0	Component (Dynamic Library)	Ship
⚠	⊙	Apache Jakarta Commons IO	1.1	Apache License Version 2.0	Component (Module)	Ship
⚠	⊙	Apache Jakarta Commons Logging	1.0.4	Apache License Version 2.0	File	Ship
	⊙	Apache Lucene Java	1.4.3	Apache License Version 2.0	Component (Merely Aggregated)	Ship
	⊙	Apache ORO	Unspecified	Apache 1.1	File	Ship
	⊙	Apache Xerces Java XML Parser	2.3.0	Apache 1.1	Prerequisite (Separate Work)	Used at runtime
	⊙	bcrypt - blowfish file encryption	1.1	BSD 2.0	Snippet	Ship
⚠	⊙	cryptlib	Unspecified	Cryptlib License (Sleepycat License +)	Snippet	Ship
	⊙	db-charmer	1.6.10	MIT License V2	File	Ship
⚠	⊙	GnuPG	1.2.4	GPL 3.0	File	Ship

⚠ Flags Indicate Potential License Conflicts

[Drill Downs](#) Links To Conflict Details




License Conflict Process

GPL 3.0 License

— Your Right to Distribute Source Code / Enforced Sharing of Source —

☐ True	You may distribute source code.
☐ False	
☒ True	You are required to distribute source code.
☐ False	

You are required to distribute the source code of the Work Based on the Licensed Code.

Proprietary Commercial License

— Your Right to Distribute Source Code / Enforced Sharing of Source —

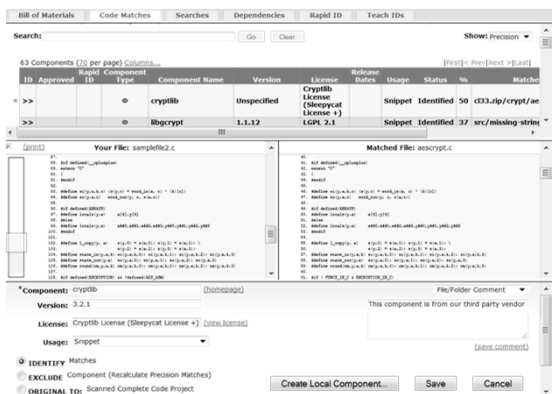
☐ True	You may distribute source code.
☐ False	
☐ True	You are required to distribute source code.
☒ False	

You are not entitled to distribute source code.

Conflicts Display Which License Obligations Are In Contention




Code Identification & Resolution



Assign Source Code And Binaries to OSS Projects

Link Code To OSS Metadata

- License
- Version
- Usage
- Comments
- Homepage
- Approval Status



Reporting

Customizable Reporting

Select a Report Template: Summary

Report Title: Summary

Report Header:

Select Report Sections:

- Summary
- Analysis Summary
- Bill of Materials
- Licenses in Effect
- License Conflicts
- Potential Bill of Materials
- IP Architecture
- Obligations
- File Inventory
- Identified Files
- Excluded Components
- Overview

Summary

Analysis Summary

Bill of Materials

Licenses in Effect

License Conflicts

Potential Bill of Materials

IP Architecture

Obligations

File Inventory

Identified Files

Excluded Components

Overview

HTML

Open Office

MS Word

MS Excel

Table with 5 columns: Component, Version, License, and others. Rows include Apache Commons Logging, Apache Commons IO, etc.

Table with 2 columns: Component, Version. Rows include Apache Commons Logging, Apache Commons IO, etc.



Code Label

Code Label

Sendmail 8.12.11

Code Base 5.870MB

% Content

Total Open Source 3.244MB 55%

Reciprocal as Components 0MB 0%

Reciprocal as Files 0MB 0%

Permissive 3.244MB 55%

Owned 0MB 0%

Total Proprietary 2.626MB 45%

Licensed 3rd Party 0MB 0%

Owned 2.626MB 45%

Total Unknown 0MB 0%

BSD 2.0 <1%

GPL 2.0 [modified] <1%

Sendmail License 55%

[template] Basic Proprietary Commercial License 45%

Cannot be used for purposes beyond Internal Production Use

Print Code Label

Components: FreeBSD*, Sendmail, Server Resources Server Suite*

*Indicates Partial Component

Furnished by: Unknown

Powered by Black Duck Software

 **BLACKDUCK**

 **ManageWare**
THINK Beyond

Using Black Duck

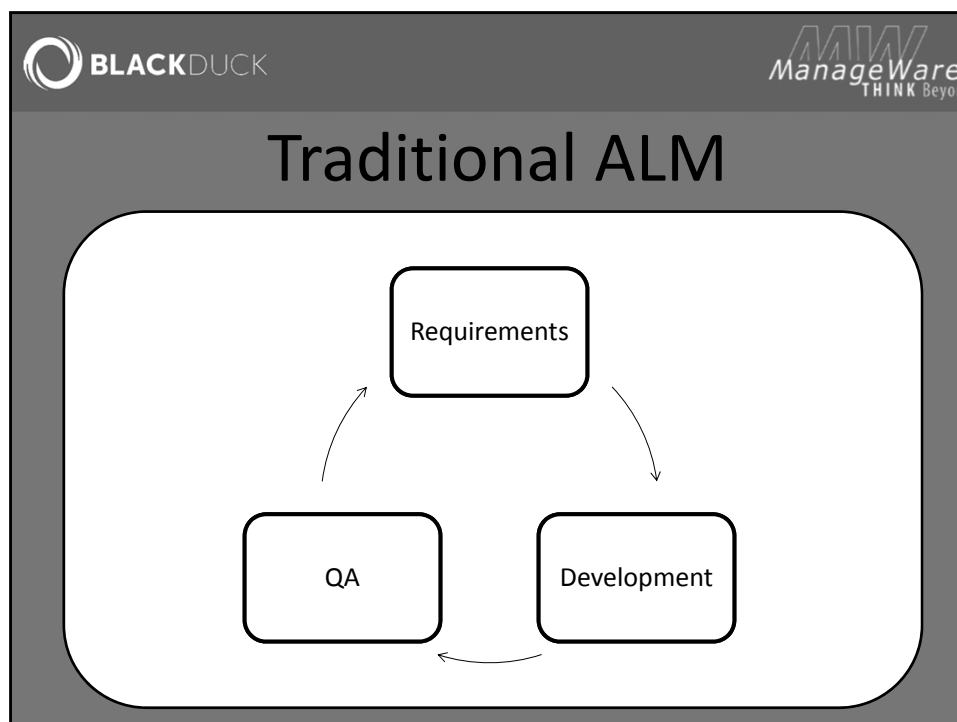
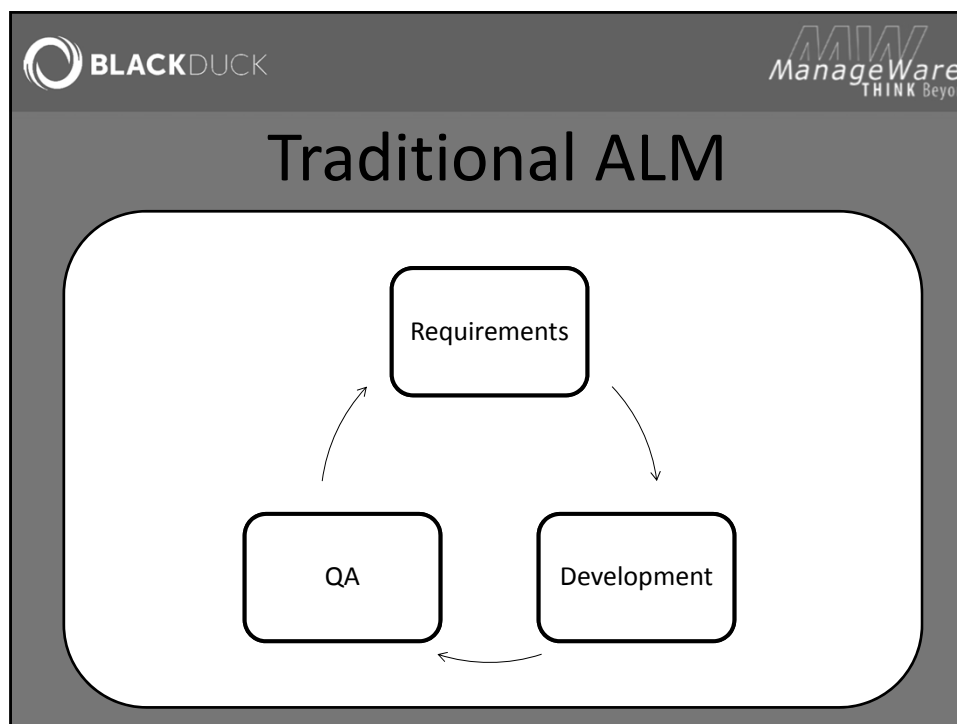
- **Acquire, Scan, Analyze and Validate FOSS and other Code**
Make better choices acquiring code
- **Configurable Approval Workflow**
Accelerates approval process
- **Catalog Components**
Catalog of approved components saves time, eliminates duplicate requests/redundant effort
- **Manage Security Vulnerabilities**
Ensures selection and use of most secure FOSS components
- **Index Code, Code Search**
Increase developer productivity

 **BLACKDUCK**

 **ManageWare**
THINK Beyond

Benefits

- Improved development flexibility and innovation with FOSS
- Ensures best FOSS is selected and used
- Identifies risks & unknowns early in the process
- Secures alignment with key stakeholders
- Focuses on key capabilities & resources required
- Leverages years of proven, industry best practice



**BLACKDUCK**

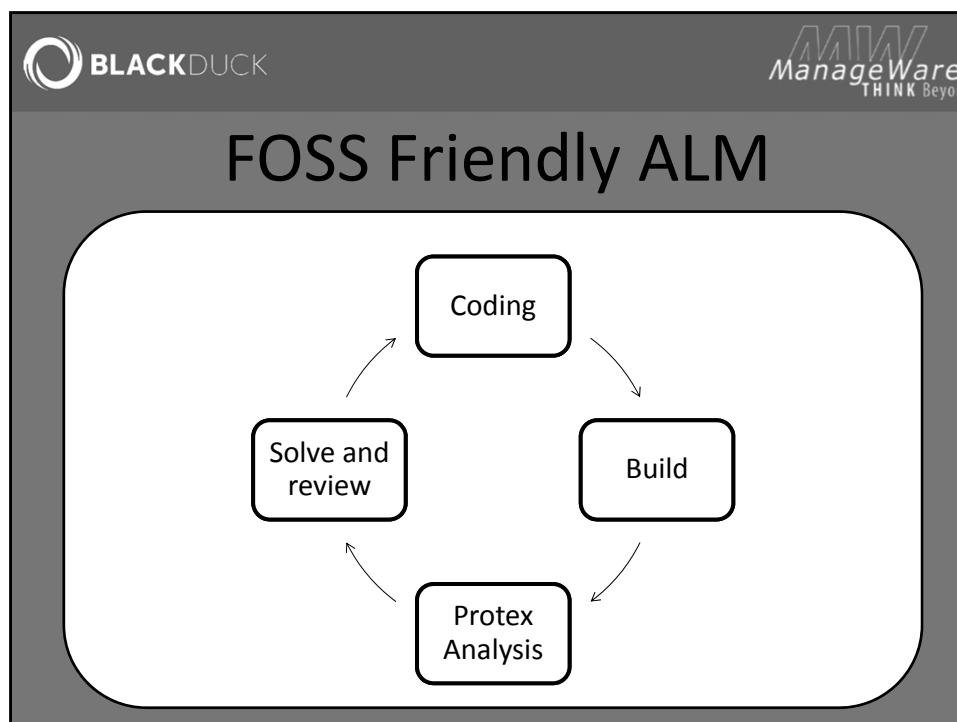
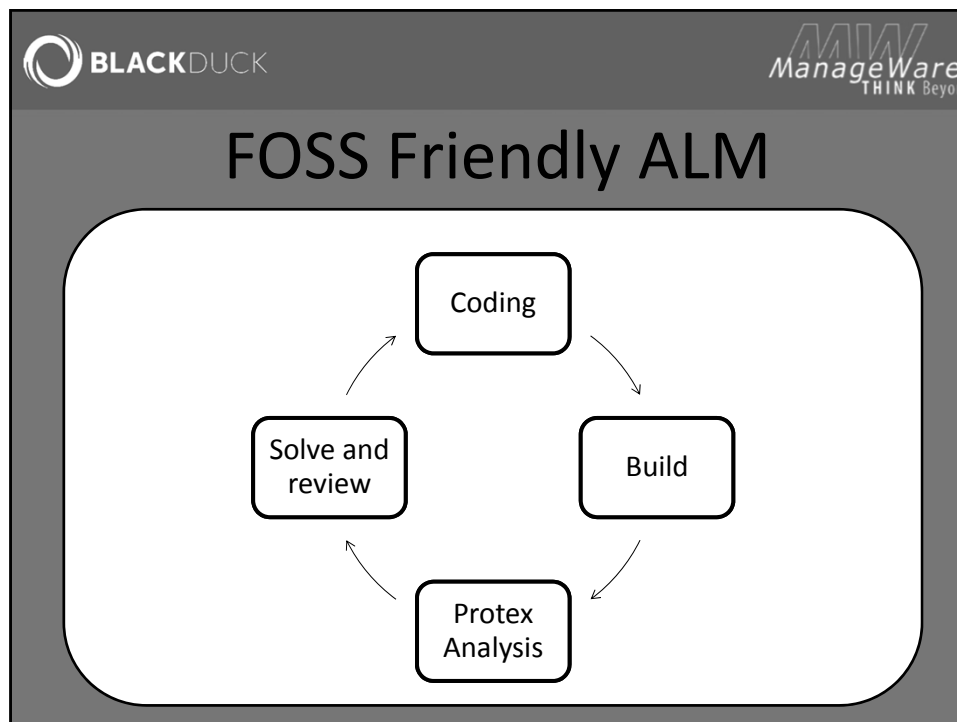
Adding OSS – No Governness

- Developer searches for component by himself
- Developer chooses code by himself
- Developer notifies legal (hopefully)
- Policy in place – Time consuming + no way to validate the developer actually adhered to the policy (taking into regards that the OSS license in the component actually is relevant)
- No Policy – even worse

**BLACKDUCK**

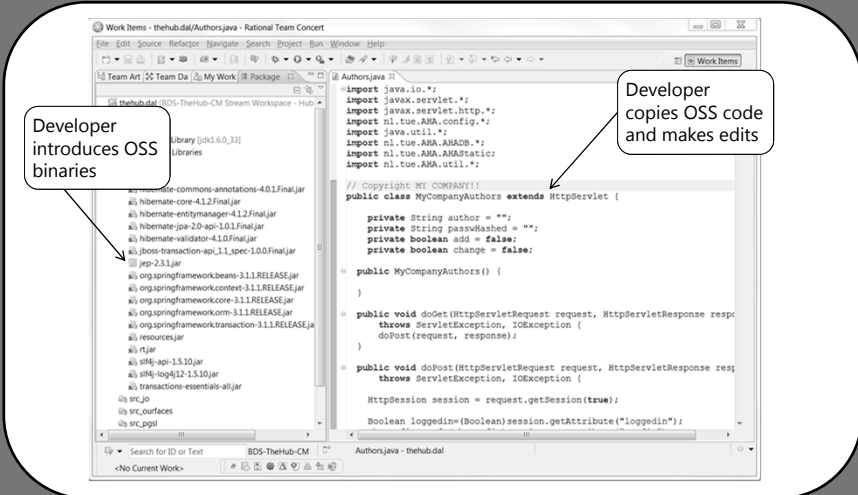
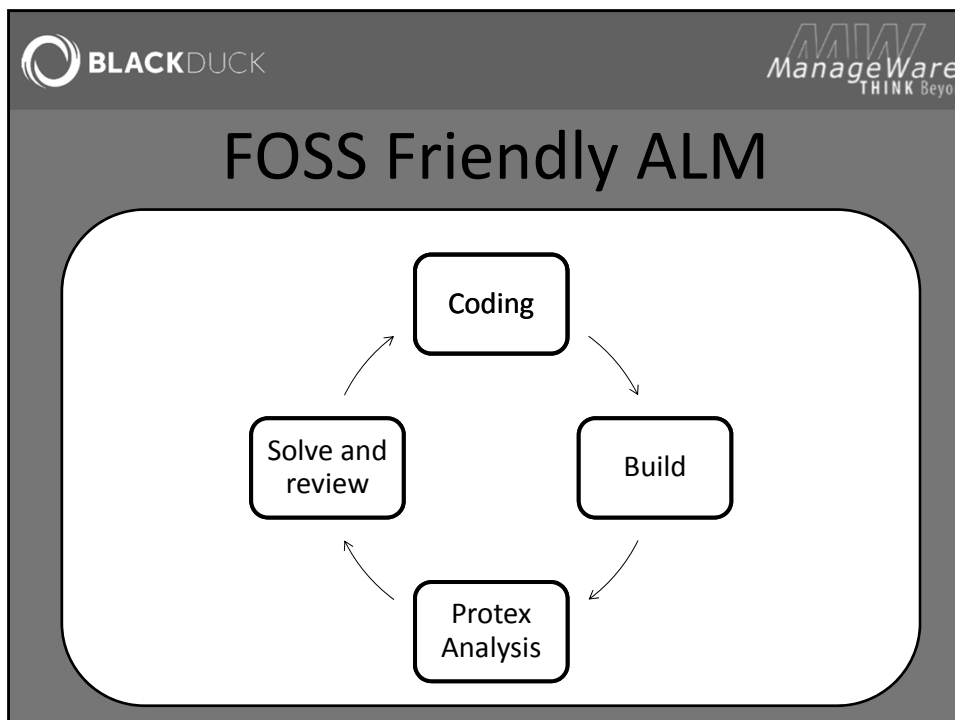
Outcome – No Governness

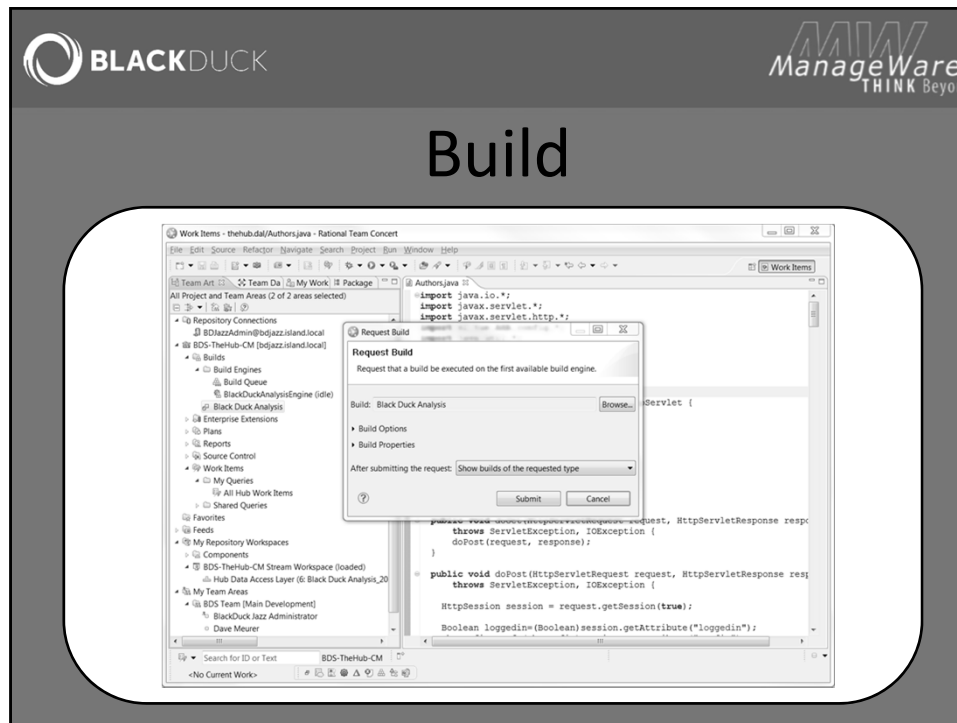
- Several product branches to maintain
- Not the best fit / solution is chosen
- Legal liability






Coding

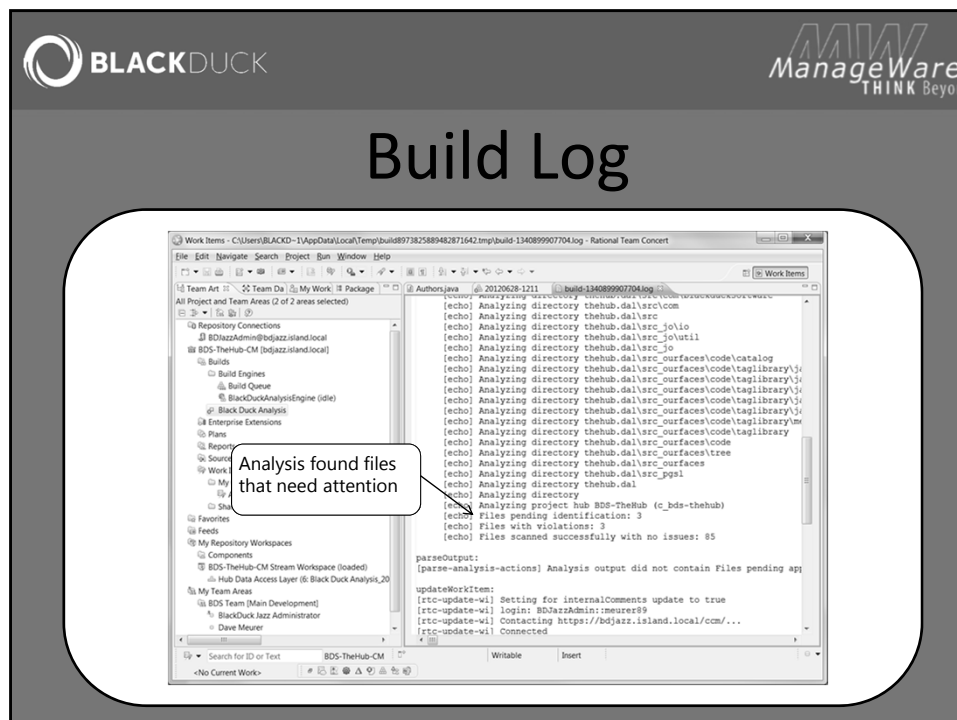
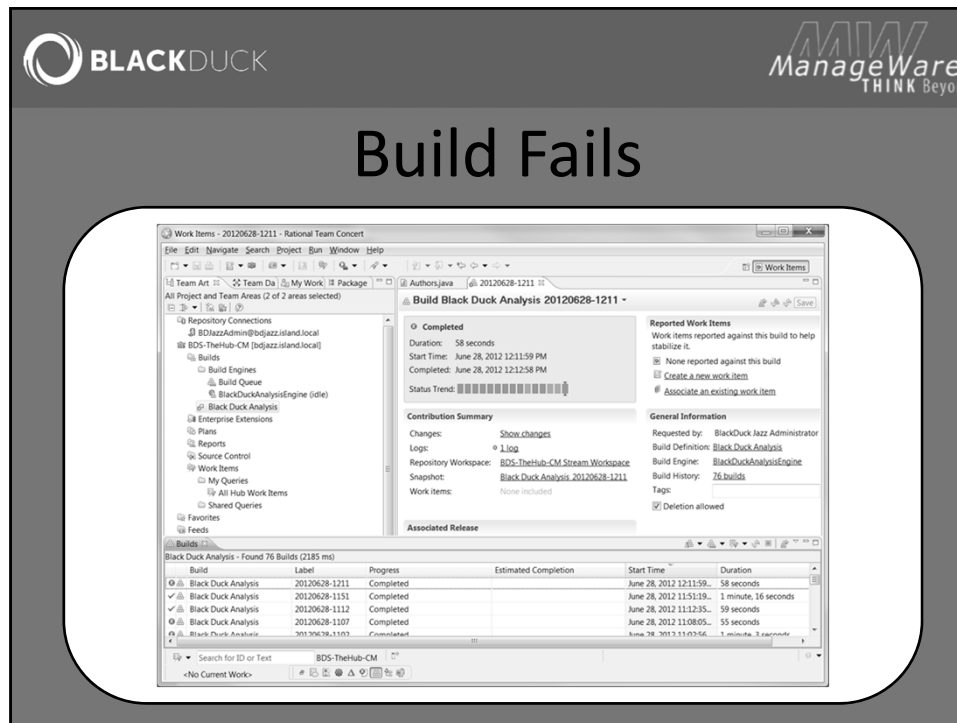







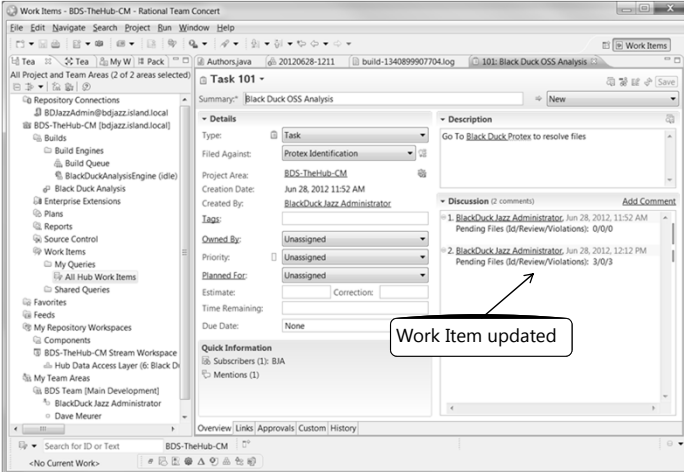

Centralized Analysis

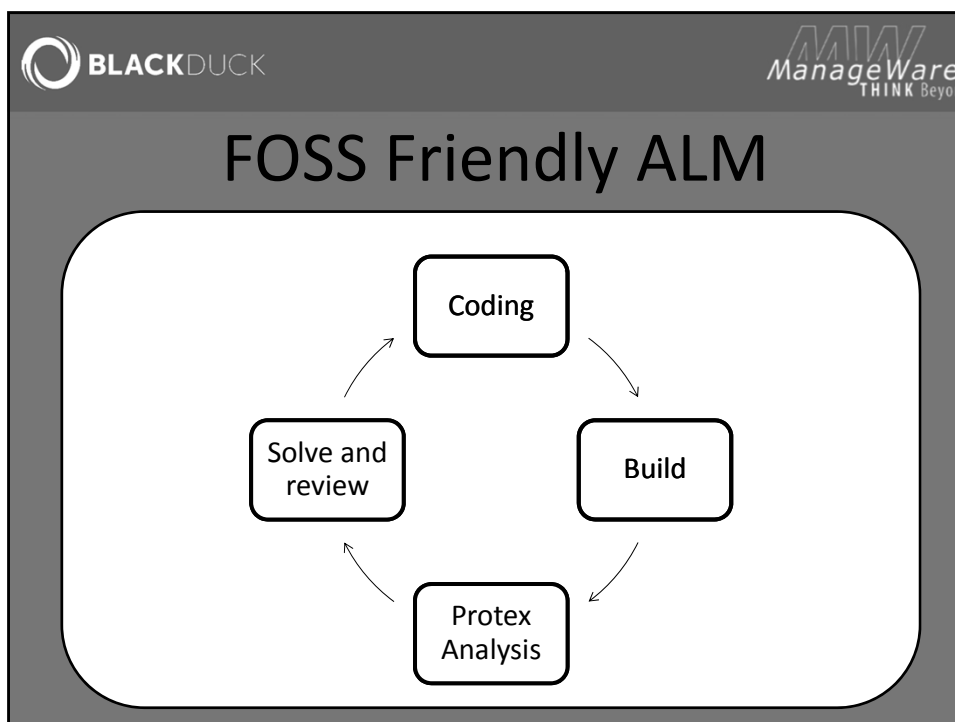
- CM integration: SVN, Git, RTC...
- 100% view into the Source code.
- Build systems Integration
 - Runs a BDS scan automatically
 - Gives us the ability to stop the release if certain reciprocal licenses are found (GPL3,AGPL,...)
 - Shows new issues within the build





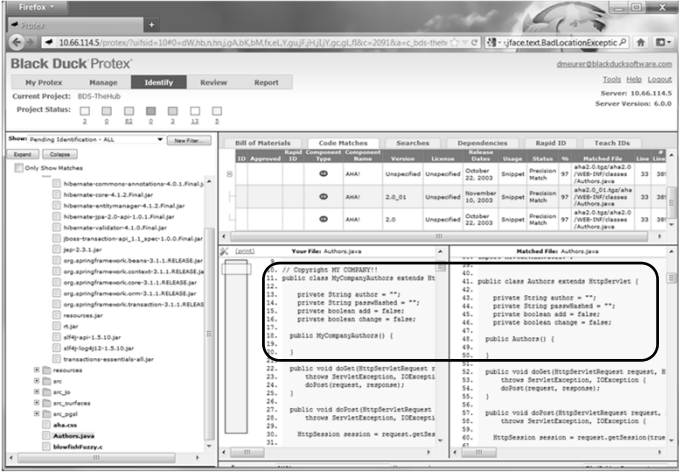

Build Log

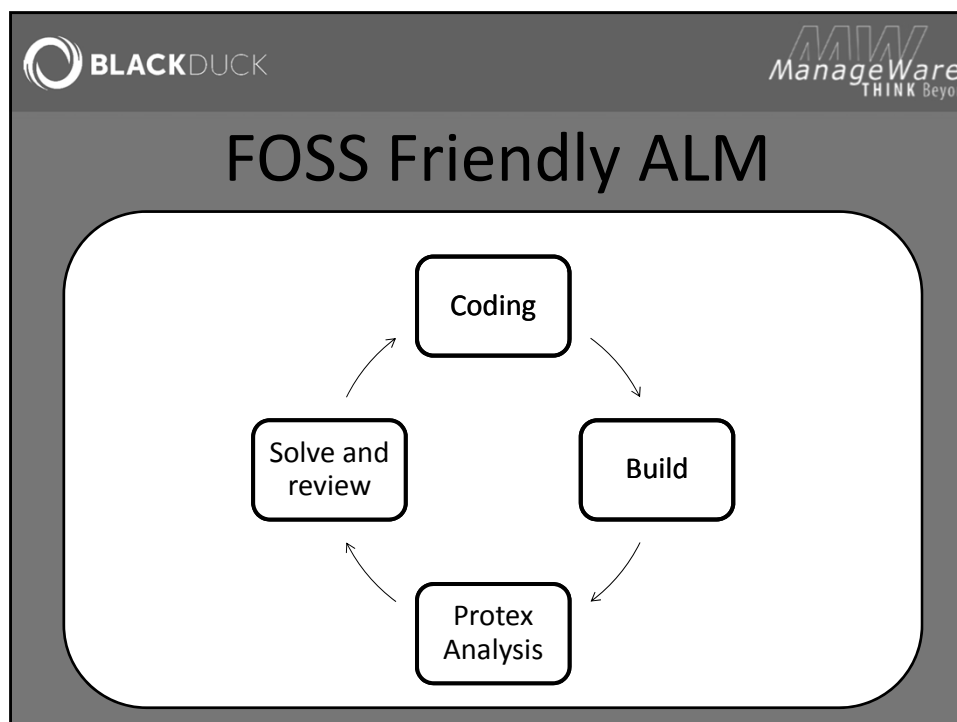







Fuzzy Snippet Matched







ManageWare
THINK Beyond

Audit : License Conflict

License Conflicts							
Component	Component Version	License	Conflicting Component	Conflicting Component Version	Conflicting Component License	Component Obligation	Conflicting Component Obligation
Linux Test Project	2004	GPL 2.0	Simple Tutorial		My Company Proprietary License	You are required to distribute the source code of the Work Based on the Licensed Code (per GPL).	You are not entitled to distribute source code.
Linux Test Project	2004	GPL 2.0	Simple Tutorial		My Company Proprietary License	You are not entitled to impose a fee related to what Recipient may do with the code.	Recipient will be expected to pay a fee.
libcrypt	1.1.12	LGPL 2.1	Simple Tutorial		My Company Proprietary License	You are required to distribute the source code of the Dynamic Library (per LGPL).	You are not entitled to distribute source code.
libcrypt	1.1.12	LGPL 2.1	Simple Tutorial		My Company Proprietary License	You are not entitled to impose a fee related to what Recipient may do with the code.	Recipient will be expected to pay a fee.



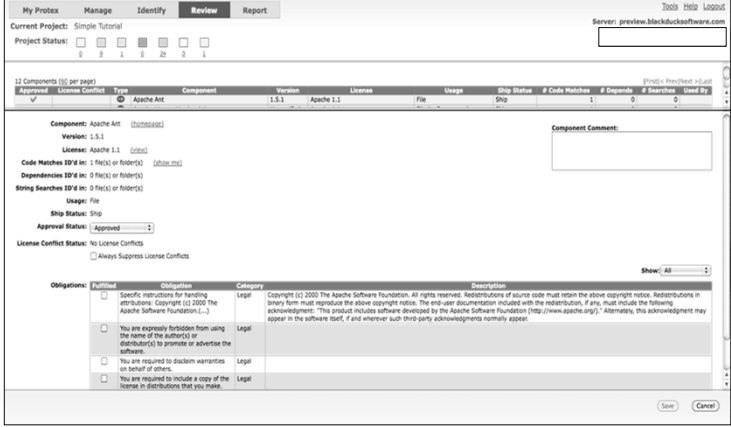
ManageWare
THINK Beyond

Audit : Obligations

Obligations					
Component	License	Fulfilled	Obligation	Category	Description
Apache Ant	Apache 1.1	No	Specific instructions for handling attributions: Copyright (c) 2000 The Apache Software Foundation (...)	Legal	Copyright (c) 2000 The Apache Software Foundation. All rights reserved. Redistributions of source code must retain the above copyright notice. Redistributions in binary form must reproduce the above copyright notice. The end-user documentation included with the redistribution, if any, must include the following acknowledgment: "This product includes software developed by the Apache Software Foundation (http://www.apache.org/)." Alternatively, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.
Apache Ant	Apache 1.1	No	You are expressly forbidden from using the name of the author(s) or distributor(s) to promote or advertise the software.	Legal	
Apache Ant	Apache 1.1	No	You are required to disclaim warranties on behalf of others.	Legal	
Apache Ant	Apache 1.1	No	You are required to include a copy of the license in distributions that you make.	Legal	
Apache Ant	Apache 1.1	No	You are required to limit the liability of others (beyond reproducing a license that contains a limitation of liability).	Legal	
Apache License Version 1.1	Apache 1.1	No	Specific instructions for handling attributions: Copyright (c) 2000 The Apache Software Foundation (...)	Legal	Copyright (c) 2000 The Apache Software Foundation. All rights reserved. Redistributions of source code must retain the above copyright notice. Redistributions in binary form must reproduce the above copyright notice. The end-user documentation included with the redistribution, if any, must include the following acknowledgment: "This product includes software developed by the Apache Software Foundation (http://www.apache.org/)." Alternatively, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.
Apache License Version 1.1	Apache 1.1	No	You are expressly forbidden from using the name of the author(s) or distributor(s) to promote or advertise the software.	Legal	
Apache License Version 1.1	Apache 1.1	No	You are required to disclaim warranties on behalf of others.	Legal	
Apache License Version 1.1	Apache 1.1	No	You are required to include a copy of the license in distributions that you make.	Legal	
Apache License Version 1.1	Apache 1.1	No	You are required to limit the liability of others (beyond reproducing a license that contains a limitation of liability).	Legal	
Apache License Version 1.1	Apache 1.1	No	Specific instructions for handling attributions: You must keep intact all the notices that refer to: (...)	Legal	<p>You must keep intact all the notices that refer to this License. <p> <p> Use this text in the source code: one line to give the library's name and an idea of what it does. Copyright (C) year name of author <p> <p> This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the license, or (at your option) any later version. <p> <p> This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details. <p> <p> You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA<p> <p> <p>
Binbase Cluster System - cluster	GPL 2.1	No	Specific instructions for handling modifications: You must cause the files modified to carry prominent notices...	Legal	You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.
Binbase Cluster System - cluster	GPL 2.1	No	Terms for distribution of source code - Offer for distribution of source code must be valid for 3 years.	Legal	Offer for distribution of source code must be valid for 3 years.




Audit : Tracking Fulfilments



The screenshot shows the 'Review' tab of the Black Duck Audit interface. It displays details for the 'Apache Ant' component, including its version (1.5.1), license (Apache 1.1), and usage (File). The interface includes sections for 'Code Matches', 'Dependencies', 'String Searches', and 'Ship Status'. There is also a 'Component Comment' field and a 'Show' dropdown menu.




Conclusion

- Integration with your SCM, Build, IDE
- Run automatically from your build system
- Fail the build upon critical violations
- Create a work items regarding the violations
- Provide insight about conflict with OSS policy
- Address contentious license ASAP
- Recheck the cycle



