FOSS Governance Best Practices

2011 FOSS Con, Korea

November, 2011

Phil Odence
VP of Business Development
Black Duck Software

Black Duck Software

Enabling Multi-Source Development at Enterprise Scale

Managing FOSS Abundance

- Over **550,000** projects
- **85%** of enterprises use OSS
- **>60%** lack policy, automation

THE LINUX FOUNDATION

Black Duck Koders.com

ohloh

olliance group
a blackduck company

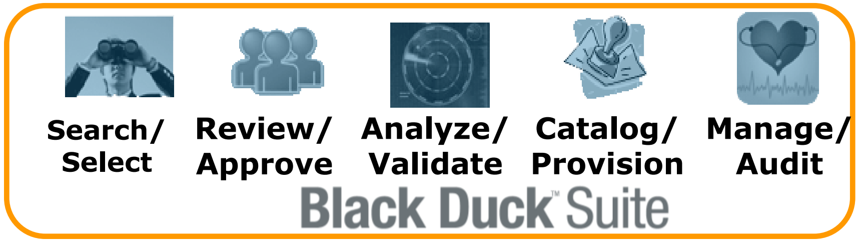
eclipse FOUNDATION MEMBER

Vision: The Vendor that….

- **Organizations** trust for management of FOSS in product app development
- **Developers** seek out as trusted source of FOSS knowledge

Enterprise-Scale Solution

- Automates FOSS Management



1000 Customers in 24 Countries

CISCO, intel, Motorola, JBoss, Bank of America, LUCASFILM Ltd, RIM, accenture, Fidelity INVESTMENTS, SAP, YAHOO!, ORACLE, sas, Allstate. You're in good hands., ADP, LG, THOMSON

blackduck

Know Your Code.

First of all…

"Software is Eating the World"

Marc Andreessen

Wall Street Journal

And the world is hungry for FOSS…

Accenture: 73% of respondents: Open source is changing the way business operates IT

Forrester: "When it comes to Enterprise IT adoption, Open Source Has 'Crossed the Chasm'"; 79% of IT developers use open source in their development projects

IT Development Benefits and Challenges with FOSS

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

Gartner

- Key Benefits
  - Flexibility
    - Modify, mix, reuse code
  - Innovation
    - Leverage OSS and community
  - Cost Optimization
    - Reduce or eliminate acquisition costs

- Challenges
  - Technical Failure
    - Operational exposure
    - Needs to be audited, managed
  - Security Risks
    - Business exposure
  - IP Risks
    - Legal exposure

Source: Mark Driver, Gartner Group, November 2010

Baseline Requirements for World-Class FOSS Management & Governance

Strategy

- Articulate the business objectives for use of FOSS

Policy

- The rules for evaluating, approving, using and releasing FOSS code and participating in communities

Processes & Tools

- Embed the policy in the day to day

FOSS Process Maturity Model

	Exposed	Measured	Managing	Participating	Driving
Discovery	• No formal guidelines or processes	• Some guidelines provided	• Clear policy on acceptable sources and attributes; • Developers educated	+Tools to facilitate search and verification of attributes	+Participation in key communities to drive company's requirements
Review and Selection	• ad hoc	• Incorporated components are identified and tracked	• Clear policy and process; • Oversight and exception handling by review board	+Automated process insuring compliance	+Active involvement with key communities creates responsive FOSS supplier relationships
Code Management	• FOSS included and managed with proprietary code	• FOSS is tracked separately	• Policy establishes owner and responsibilities for each component; • FOSS repository; • Use tracking	+Automated process tracks sources, attributes, use and compliance requirements	+FOSS repository extended to support external releases
Maintenance and Support	• ad hoc	• Some approach to stay abreast of bug fixes and new releases	• Policy defines responsibilities for each component owner; • Consolidated support model	+Automated process tracks issues, fixes, versions	+Support model extended externally; +Automated process extended to handle external support
Compliance Program	• ad hoc, if any	• Incorporated FOSS components listed for each release; • Compliance requirements assembled by hand	• Review and code management processes prevent surprises; • Automated audit of product releases; • Compliance process with reporting	+Automated process integrates review, code management and compliance functions; +Automated reporting for management and customers	+Policy and automated process for audit and review of contributions
Community Interaction	• Download code	• Download code	• Download code; • Track updates; • Participate in forums *without* company identification	+Participate in forums *with* company attribution; +Contribute bug fixes	+Contribute new projects/components; +Sponsor key communities
Executive Oversight	• Probably none	• Executives receive lists of FOSS components in use	• Legal & line-of-business management participation on review board	+Policy for community participation; +Process for contribution of bug fixes	+Policy and process for contributing components, sponsorship for projects

Discovery Best Practices

- Provide guidelines that include use, license and other aspects
  - Avoid wasting time on choices that will not be approved
  - Leverage code that the organization has experience with
- Provide broad training that lets developers understand importance
- Automate with tools that augment training
- Participate in communities (internal and external) around key components to drive direction

- Case Study
  - Large investment firm
    - Very limited, approved stack
  - Global Defense Contractor
    - Less limited, much more training
    - More tools (like Ohloh) required
    - Equipped 10Ks developers

Know Your Code.

Review and Approval Best Practices

- Require every new use of a FOSS component be reviewed and approved
- Establish an Open Source Review Board
- Train developers to provide complete information and sensitize approvers to urgency
- Record and make decisions visible
- Automate workflow to ensure speedy approvals and provide visibility to pipeline

- Case Study
  - Enterprise Telco Equipment Provider
    - Highly sophisticated, automated routing
      - Auto Approve, Paralegal, Lawyer
      - By division
  - Switching Equipment Provider
    - Numerical scales for “soft” attributes

Procurement Best Practices

- Evaluate and educate suppliers on your policy and processes and evaluate their governance programs
- Require suppliers to provide a complete software bill of materials specifying:
  - FOSS components
  - Usage of components
  - Licenses and copyrights; other requirements and obligations
  - Industry standard format (SPDX)
- Scan incoming code to ensure accuracy
- M&A is a special case; ensure that open source analysis is integral to due diligence process

- Case Study
  - RIM
    - Develop little software in-house
    - Educate suppliers; required BoMs
    - Require scanning on all in-coming code
  - SAP
    - Sophisticated M&A process
    - FOSS scanning; introduced early

blackduck

Know Your Code.

Code Management Best Practices

- Provide central catalog or repository separately tracking FOSS components from proprietary code
- Track component ownership, usage, and compliance requirements
- Encourage version standardization and reuse
- Automate and integrate with component approval process to minimize overhead

- Case Study
  - Large Bank
    - Broadly rolled out process
    - Requires internal search first
    - Fully integrated catalog
    - Security vulnerability monitoring

Maintenance and Support Best Practices

- Processes recognition that open source needs every bit as much support as commercial software
- Model incorporates commercial, community and internal support as appropriate
- Require support assessment and plan as part of component approval
- Loop fixes back and non-core enhancements back into project to avoid re-patching
- Assign component owners

- Case Study
  - Financial Services company
    - Systems build on Postgres
    - Hired small # of community members
    - Internal support, also leverage community
    - Outside firm (credativ) for backup
  - Switching Equipment Manufacturer
    - Individual owners in groups
    - Corporate team for cross-group components

Know Your Code.

Compliance Best Practices

- Good upstream practices should make this a “rubber stamp”
- Assemble and verify FOSS BoM for every release
- For each FOSS component, understand:
  - License & Obligations
  - How it’s linked
  - How it’s used (internal, SaaS, distributed, etc)
- Incorporate compliance verification as automated part of release process
- Be prepared to handle inquiries (LF Open Compliance Directory)

- Case Study
  - Acquired division of large sw/services company
    - Completely integrated scanning
    - Auto-generate:
      - EULA, Certificate of Origin, Obligations
  - Intel, SAP,…most Black Duck customers
    - Incorporate scanning in release process

Community Interaction Best Practices

- Regularly track each component used for
  - News
  - Level of Activity
  - Updates/New Releases
  - Security and Quality Issues
- Participate in forums, report issues and/or contribute fixes to avoid repeated patching
- Sponsor and steer project direction

- Case Study
  - IBM
    - Eclipse, Apache, Linux
  - Huawei
    - Share bug fixes with community
    - Evaluate features
  - Black Duck
    - Postgres/credativ
    - Lucine/Lucid Imagination

Executive Oversight Best Practices

- OSS Management Board (above OSRB)
  - Policy and escalations
- All executives should be familiar
- Assign an interested executive sponsor
- Regular reporting and visibility demonstrating the value of FOSS and the health of the governance program

- Case Study
  - Telco Equipment Provider
    - OSRBs for each group
    - OSMB for exceptions
    - Regular executive reports
      - Measures of dev/gov processes

Know Your Code.

Managing FOSS to Advantage

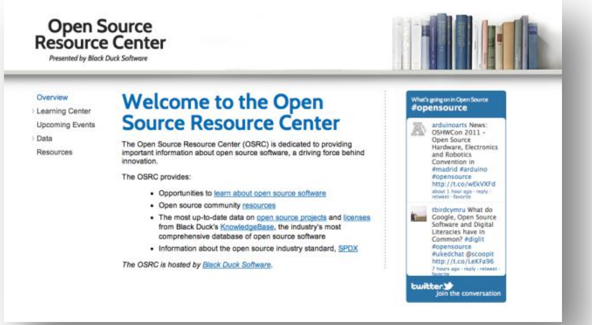
- FOSS management requires investment
- Organizations the implement best practices across all elements of maturity get the best returns

Resources and Getting Started

- Open Source Management Assessment, Policy Workshop, Process Workshop
- www.blackducksoftware.com

olliance | group

a blackduck company



Open Source Resource Center

Presented by Black Duck Software

Welcome to the Open Source Resource Center

The Open Source Resource Center (OSRC) is dedicated to providing important information about open source software, a driving force behind innovation.

The OSRC provides:

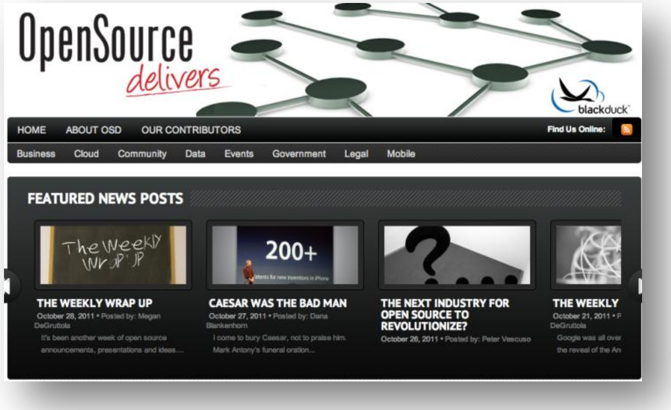
- Opportunities to learn about open source software
- Open source community resources
- The most up-to-date data on open source projects and licenses from Black Duck's KnowledgeBase, the industry's most comprehensive database of open source software
- Information about the open source industry standard, SPDX

The OSRC is hosted by Black Duck Software.

What's going on in Open Source
#opensource

arduinoarts News: OSHWCon 2011 - Open Source Hardware, Electronics and Robotics Convention in #madrid #arduino #opensource http://t.co/wEkVXFd
about 1 hour ago · reply · retweet · favorite

tbirdcymru What do Google, Open Source Software and Digital Literacies have in Common? #diglit #opensource #ukedchat @scoopit http://t.co/LeKFa96
7 hours ago · reply · retweet · favorite



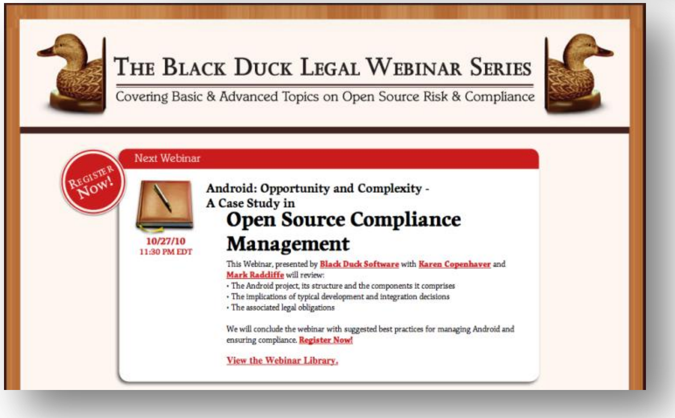
FEATURED NEWS POSTS

THE WEEKLY WRAP UP
October 28, 2011 • Posted by: Megan DeGruttola
It's been another week of open source announcements, presentations and ideas....

CAESAR WAS THE BAD MAN
October 27, 2011 • Posted by: Dana Blankenhorn
I come to bury Caesar, not to praise him. Mark Antony's funeral oration...

THE NEXT INDUSTRY FOR OPEN SOURCE TO REVOLUTIONIZE?
October 26, 2011 • Posted by: Peter Vescuso

THE WEEKLY
October 21, 2011 • P
DeGruttola
Google was all over
the reveal of the An



THE BLACK DUCK LEGAL WEBINAR SERIES

Covering Basic & Advanced Topics on Open Source Risk & Compliance

Next Webinar

10/27/10
11:30 PM EDT

Android: Opportunity and Complexity - A Case Study in

Open Source Compliance Management

This Webinar, presented by Black Duck Software with Karen Copenhaver and Mark Radcliffe will review:
- The Android project, its structure and the components it comprises
- The implications of typical development and integration decisions
- The associated legal obligations

We will conclude the webinar with suggested best practices for managing Android and ensuring compliance. Register Now!

View the Webinar Library.