

blackduck

Automated Solutions for Software IP Risk Management

# Working with Open Source - Software Compliance Management



blackduck

**Karen Faulds Copenhaver**
**EVP & GC Black Duck Software, Inc.**

Black Duck Confidential
Copyright © 2004 Black Duck Software, Inc. All Rights Reserved.

# Open Source Myth No. One

From those fond of the discussion of deadly diseases:

*You cannot use open source software in a proprietary environment [or you will die].*

Black Duck Confidential
Copyright © 2004 Black Duck Software, Inc. All Rights Reserved.

# Open Source Myth No. Two

From those who like to keep it simple:

*All open source licenses require the release of source code for everything.*

Black Duck Confidential
Copyright © 2004 Black Duck Software, Inc. All Rights Reserved.

# Open Source Myth No. Three

From those who like to live one day at a time:

*We don't have to worry about open source as long as we are only using it internally.*

Black Duck Confidential
Copyright © 2004 Black Duck Software, Inc. All Rights Reserved.

# Open Source Myth No. Four

From those who think those were the good old days:

*The easiest answer is to*

*“just say no.”*

Black Duck Confidential
Copyright © 2004 Black Duck Software, Inc. All Rights Reserved.

# Open Source Myth No. Five

From those who enjoy bad lawyer jokes:

*None of these agreements are enforceable so it doesn't really matter anyway.*

Black Duck Confidential
Copyright © 2004 Black Duck Software, Inc. All Rights Reserved.

# Open Source Myth No. Six

From those who still believe in knights in shining armor:

*Now that the big guys have joined the party, they will make the world safe for open source.*

Black Duck Confidential
Copyright © 2004 Black Duck Software, Inc. All Rights Reserved.

# Open Source Myth No. Seven

From those who never got caught smoking in the bathroom in high school*:*

*No one will ever know.*

Black Duck Confidential
Copyright © 2004 Black Duck Software, Inc. All Rights Reserved.

# Open Source Myth No. Eight

From those who retain their utopian optimism:

*It doesn't matter! Eventually everything will be open source and all VCs and proprietary software will have disappeared off the face of the earth.*

Black Duck Confidential
Copyright © 2004 Black Duck Software, Inc. All Rights Reserved.

# Open Source Myth No. Nine

From those who enjoy a good conspiracy theory:

*The SCO lawsuit will resolve all of these issues.*

Black Duck Confidential
Copyright © 2004 Black Duck Software, Inc. All Rights Reserved.

# Open Source Myth No. Ten

From those who have given up on flipping your mattress quarterly and flushing your water heater annually:

*If I even begin to think about all of these obligations, I will give up. To survive, you have to accept some risks and just move on.*

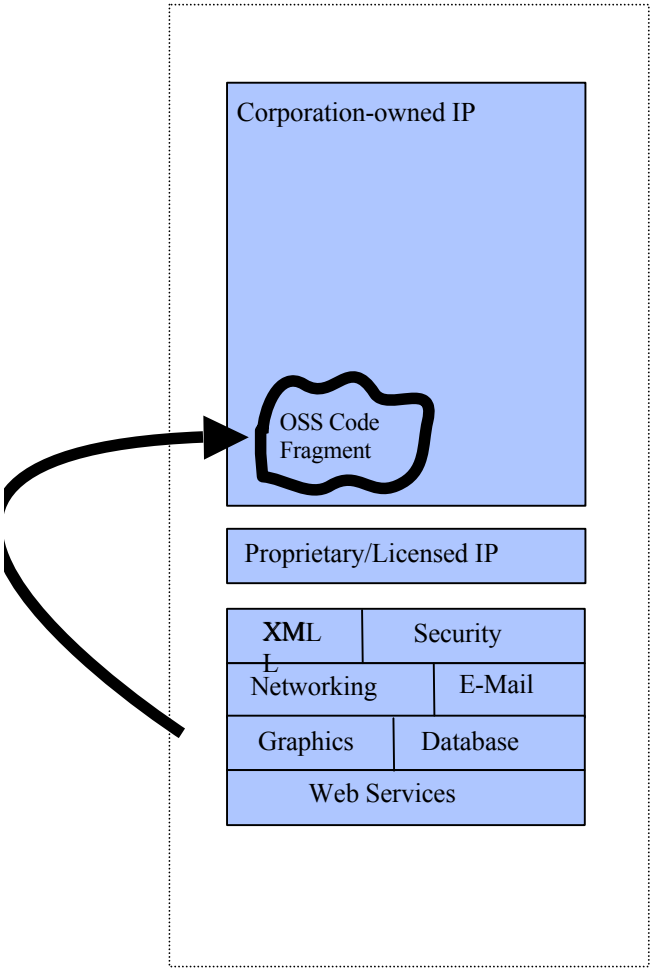
Black Duck Confidential
Copyright © 2004 Black Duck Software, Inc. All Rights Reserved.

# Open Source Software

- In this presentation I will use the term open source to refer to any software that is made widely available in source code form
- Open source software comes in many forms and is subject to many different license obligations
- We are concerned with fulfillment of the obligations imposed by the software copyright owner

Black Duck Confidential
Copyright © 2004 Black Duck Software, Inc. All Rights Reserved.

# The Mixed IP Environment




Virtually all companies that develop software are now working in a “mixed-IP environment”

- Software is created on ever increasing layers of previous work
- Reuse of internally and externally available source code is inevitable

Black Duck Confidential
Copyright © 2004 Black Duck Software, Inc. All Rights Reserved.

# Use of OSS in the Enterprise

- Time
- Cost
- Reliability
- Functionality
- Standards
- Control
- Independence
- Recruiting

Black Duck Confidential
Copyright © 2004 Black Duck Software, Inc. All Rights Reserved.

# Issues Not Unique to OSS

- Why are compliance concerns so often raised in relation to open source software?
  - Absence of control over code available for download without charge
  - Assumption that licenses unenforceable
  - Absence of honest communication between developers and management
  - Quality of source makes re-use enticing
  - Fear of delay caused by inefficient legal review

Black Duck Confidential
Copyright © 2004 Black Duck Software, Inc. All Rights Reserved.




# Writing Contract vs. Writing Code

- Need export clause
- Under time pressure
- Need to be efficient to manage cost
- Seems like waste of time to read regs
- Want to move on to harder / more interesting / higher level issues
- Want a clause from good source
- Want one that has been peer reviewed

Black Duck Confidential
Copyright © 2004 Black Duck Software, Inc. All Rights Reserved.

# Your defense?

- Cut and pasted from middle of contract and didn't notice copyright notice
- Assume copyright doesn't apply because purely functional
- Assume no one would ever enforce copyright on contract
- Can't meet deadline if don't reuse components
- Too expensive to start with a clean sheet of paper

Black Duck Confidential
Copyright © 2004 Black Duck Software, Inc. All Rights Reserved.

# Proprietary Code: Same Issues

- FOSS has made source code less sacred
  - Proprietary source is now more commonly distributed and available
- Control issues going forward will be the same for FOSS and Proprietary Source
  - FOSS compliance will be EASIER than proprietary compliance
- Likelihood of enforcement far higher for proprietary code
  - Same remedies apply

Black Duck Confidential
Copyright © 2004 Black Duck Software, Inc. All Rights Reserved.

# Software Compliance Management

- Knowing what is in the code base
  - Controlling the introduction of licensed materials into the code base
- Knowing what obligations are related to the use of licensed materials
  - Managing fulfillment of obligations
- Knowing whether the license obligations for combined components are compatible
  - Managing process from product architecture through deployment

Black Duck Confidential
Copyright © 2004 Black Duck Software, Inc. All Rights Reserved.

# Is This a Compelling Concern?

- Portfolio companies facing extensive due diligence reviews
- Public companies in compliance frenzy
- Strategic partners want more than words
- Customers seeking further assurances
- Necessary to register copyright
- Employees know more than management
- Trial by press
- Shareholder suits

Black Duck Confidential
Copyright © 2004 Black Duck Software, Inc. All Rights Reserved.

# So what's the game plan?

- Assess the code base
- Remediation
- Evaluate the process that is in place
- Roll out compliance program
- Establish due diligence policy
- Implement automated and auditable business controls

Black Duck Confidential
Copyright © 2004 Black Duck Software, Inc. All Rights Reserved.

# Conducting an Investigation

- Why might you want to take steps to preserve privilege?
  - Easier if every note is not an admission
  - Questionnaires, interim processing and preliminary conclusions
  - A lot of inaccurate information will be generated in any investigation
  - Technical jargon and analogies make misunderstandings likely

Black Duck Confidential
Copyright © 2004 Black Duck Software, Inc. All Rights Reserved.

# Privilege Considerations

- Who is conducting the investigation?
- Who has requested the investigation?
- Why was the investigation requested?
- Who is involved in the investigation?
- How is the investigation conducted?
- Is there an identified end point?
- How are the results of the investigation used?

Black Duck Confidential
Copyright © 2004 Black Duck Software, Inc. All Rights Reserved.

# Planning the assessment

- Prioritize projects
  - Do not assess entire code base at once
- Gather contextual information in advance
  - Understand what parts of the project are shipped to customers, what source code is made available to OEM partners
- Resource commitment
  - Identify resources in advance
  - Limit number of people involved
- Lay out schedule
  - Establish date for reporting to management

Black Duck Confidential
Copyright © 2004 Black Duck Software, Inc. All Rights Reserved.

# Conducting the Assessment

- Finish one project before beginning another
  - Will learn a lot in the first project
  - Avoid having too many issues swirling at once
- Triage
  - Do not let the perfect be the enemy of the good
- Stay the course
  - Do not start and stop

Black Duck Confidential
Copyright © 2004 Black Duck Software, Inc. All Rights Reserved.

# During Assessment

- Avoid disruption of development
  - Enticing to include best developers in remediation plans
- Anticipate employee concerns
  - Obligations to open source community difficult to understand
  - Not just legal obligations, moral obligations, sense of fundamental fairness
- Consider whistleblower implications

Black Duck Confidential
Copyright © 2004 Black Duck Software, Inc. All Rights Reserved.

# Remediation

- Line up legal resources in advance
  - Have sufficient technical knowledge to talk with developers directly
  - Have historical perspective on open source
  - Have knowledge of community consensus
  - Have knowledge of where repositories of information are located
  - Have contacts in the community that could be called upon for clarification anonymously

Black Duck Confidential
Copyright © 2004 Black Duck Software, Inc. All Rights Reserved.

# Remediation

- Win the right hearts and minds before charting a course of action
  - Avoid mandating a course of action constructed entirely by lawyers
  - Options will not be fully explored until there is a consensus that the issue must be addressed
  - Will always involve painful re-direction of valuable resources
  - Will not be supported unless importance and contribution are recognized

Black Duck Confidential
Copyright © 2004 Black Duck Software, Inc. All Rights Reserved.

# Remediation

- Most difficult issue is code that has been distributed to third parties
  - Obligation to notify third party?
- Understand
  - Third party's use of / redistribution of code
  - Third party's obligation to install updates
  - Reps, warranties, indemnities in agreement
- Noisy withdrawal does not benefit anyone
  - Thorough preparation extremely important
  - Focus on compliance going forward

Black Duck Confidential
Copyright © 2004 Black Duck Software, Inc. All Rights Reserved.

# Closure

- Report to management on pre-established date
  - Don’t provide preview
- Report on issues requiring continued remediation efforts
- Come prepared with specific, fully developed recommendations for remediation
  - And alternatives
- Avoid hiatus during which management knows of risk but has no plan to address

Black Duck Confidential
Copyright © 2004 Black Duck Software, Inc. All Rights Reserved.

# Evaluate Existing Processes

- Formal and informal
- Identify opportunities to capitalize on good things that are already happening
- Assess attitudes
- Identify resources/champions
- Gather lore
- Involve financial compliance experts
  - COSO
  - IT Governance Institute
    - COBIT

Black Duck Confidential
Copyright © 2004 Black Duck Software, Inc. All Rights Reserved.

# Common approaches

- Process by project
  - Developers identify open source projects that they would like to use
  - Someone – either in the legal department or an identified person in development – analyses the project for appropriateness
  - Author of open source project may be contacted
  - After it has been approved, it is placed on an internal website which indicates that it is OK to use

Black Duck Confidential
Copyright © 2004 Black Duck Software, Inc. All Rights Reserved.

# Common approaches

- Approval of licenses
  - Open source code made available under selected non-reciprocal licenses is pre-approved
  - Ignores fact that many extremely valuable projects are under reciprocal licenses and can be used without incurring obligations to release source code
  - License laundering
  - Does not consider source of the open source

Black Duck Confidential
Copyright © 2004 Black Duck Software, Inc. All Rights Reserved.

# Common approaches

- Part of final product review
  - Code is checked by QA prior to ship
  - Creates log jam
  - Few remediation options if concerns arise
  - Inevitable delay
  - Pressure to release product and fix problems later
  - Encourages better obfuscation next time

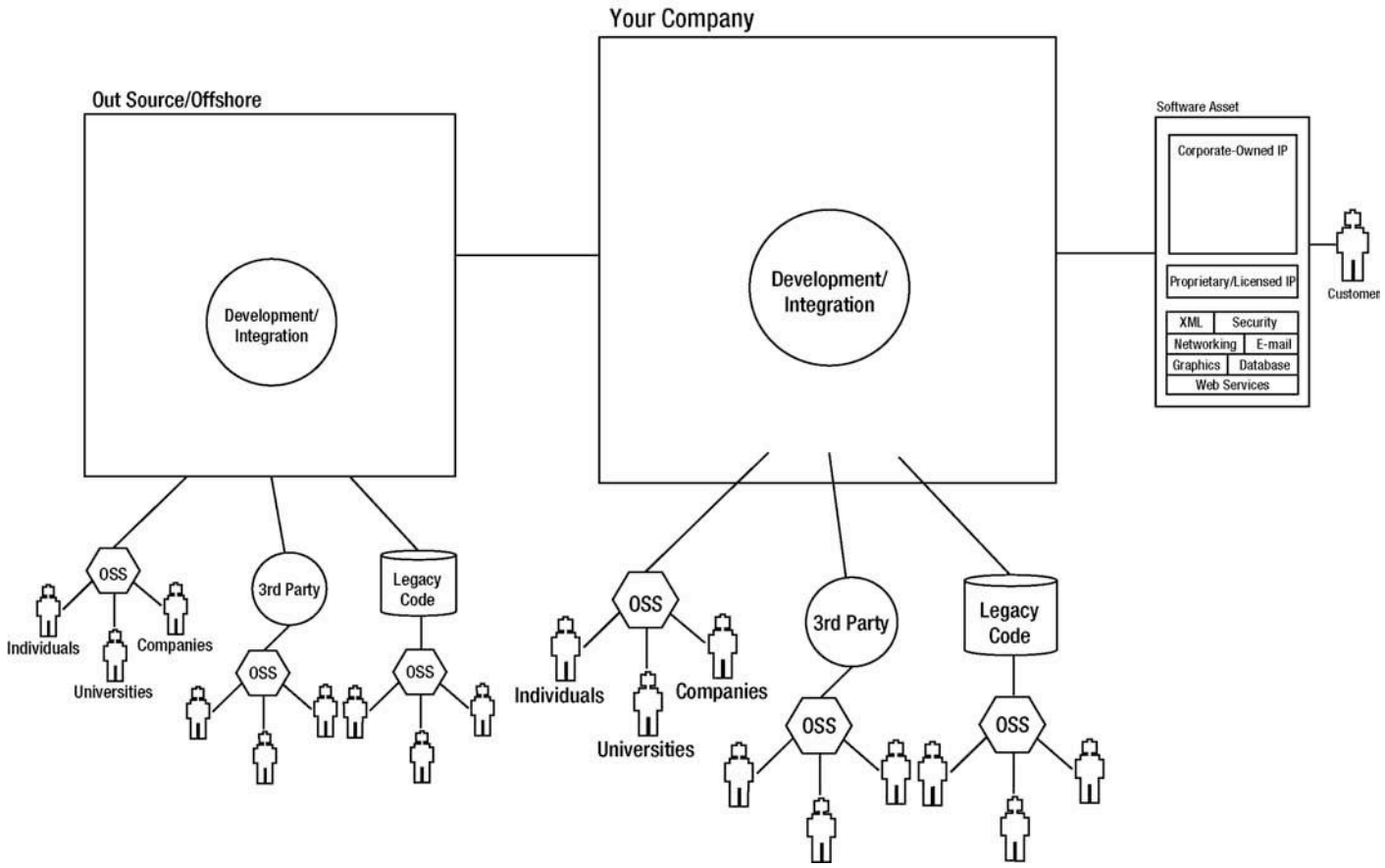
Black Duck Confidential
Copyright © 2004 Black Duck Software, Inc. All Rights Reserved.

# Ideal process

- Enables company to embrace open source
  - Sets proper tone re: compliance
  - Reduces time and cost of development
- Identifies issue early in development cycle
  - Maximize options
- Facilitates efficient engagement of legal counsel in review process
  - Gathers all available information automatically
- Efficiently tracks compliance all the way through to product ship

Black Duck Confidential
Copyright © 2004 Black Duck Software, Inc. All Rights Reserved.

# Development Environment




Black Duck Confidential
Copyright © 2004 Black Duck Software, Inc. All Rights Reserved.

# Outsourcing

- Contractual provisions to establish code pedigree
  - Assignment of intellectual property rights that is effective under local law
  - Reps, warranties and indemnities
- But concern persists
  - No personal contact
  - Concern about different cultural perspectives on importance of intellectual property rights
  - Technical solution sets tone, verifies compliance

Black Duck Confidential
Copyright © 2004 Black Duck Software, Inc. All Rights Reserved.

# Due Diligence in Transactions

- Mergers
- Acquisitions
- Spin-Offs
- Joint Ventures
- Strategic Alliances
- OEMs
- End Users

Black Duck Confidential
Copyright © 2004 Black Duck Software, Inc. All Rights Reserved.

# Post Bubble Due Diligence

- In the bubble
  - Due diligence necessary precursor to inevitable closing
- Post bubble
  - Due diligence a part of the valuation process
  - Due diligence might result in a decision not to go forward
  - Going forward with acquisition after full, unprivileged investigation results in knowledge of compliance issues is not ideal

Black Duck Confidential
Copyright © 2004 Black Duck Software, Inc. All Rights Reserved.

# Due Diligence Procedures

- Executive Interviews
- Drafts of Reps and Warranties
- Checklists
- Certificates of Originality
- Code Scans
- Development Interviews
- Preparation of Schedules
- Remediation Plans
- Escrows/Hold Backs

Black Duck Confidential
Copyright © 2004 Black Duck Software, Inc. All Rights Reserved.

# Due Diligence Sensitivities

- Intended use of code base
  - Temporarily filling hole in product line
  - Merging code bases
  - New line of business
- Make versus buy analysis
- Sophistication of acquirer
  - Early adopter of open source
  - Current policies prohibit use of open source

Black Duck Confidential
Copyright © 2004 Black Duck Software, Inc. All Rights Reserved.

# Remediation

- Remediation plan
  - Further research of options
  - Removal of code
  - Restructuring of architecture
  - Issuing patch
  - Releasing source code
- Timing
  - Delay closing / contributory infringement
  - Post closing / direct infringement

Black Duck Confidential
Copyright © 2004 Black Duck Software, Inc. All Rights Reserved.

# Role of Counsel in Compliance

- Oversee assessment of code base
- Determine if license required
  - copyrightable subject matter
  - fair use
  - de minimus (quantitative and qualitative)
- Verify applicable license
- Verify compliance

Black Duck Confidential
Copyright © 2004 Black Duck Software, Inc. All Rights Reserved.

# Role of Counsel in OS Community

- Legal opinions on derivative works?
- Development of community consensus on copyright law issues of importance to the community?
- Advocating compliance?
- Advocating abstinence?
- Consulting with experienced counsel?
- Assisting employees who want to work on open source projects to understand their obligations to the company/community?

Black Duck Confidential
Copyright © 2004 Black Duck Software, Inc. All Rights Reserved.

blackduck

"It's the alligators that you don't see that will get you."

*IT Control Objectives for Sarbanes-Oxley*
*IT Governance Institute*
*www.itgi.org*

Black Duck Confidential
Copyright © 2004 Black Duck Software, Inc. All Rights Reserved.