



Challenges In Technology Adoption & License Compliance

Douglas Levin
President and CEO
Black Duck Software



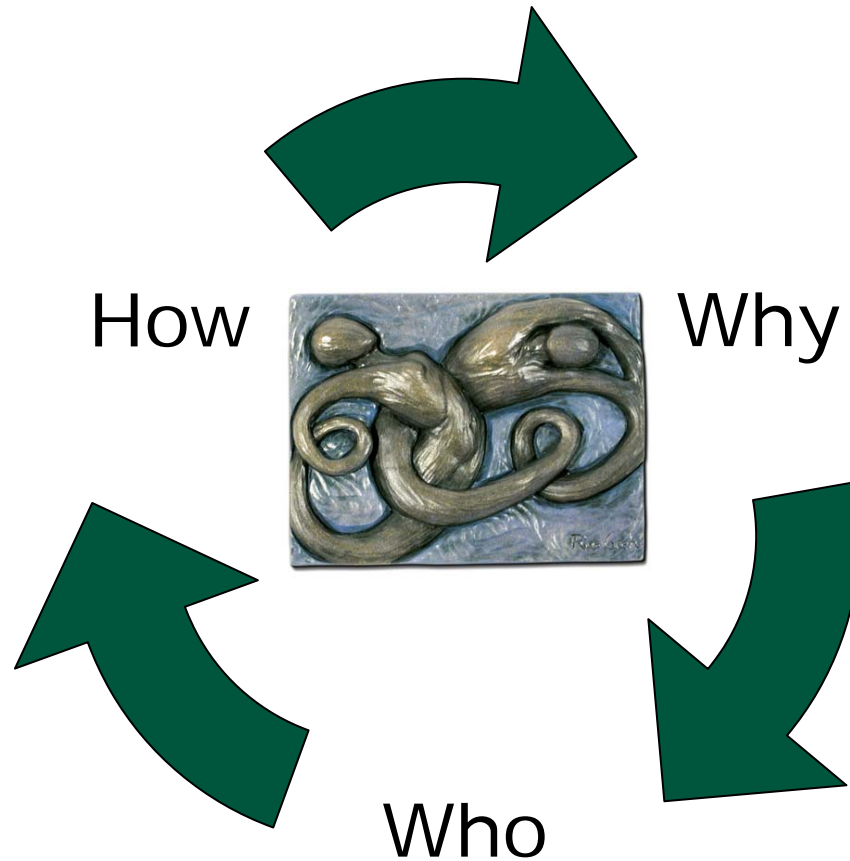
Challenges In Technology Adoption & License Compliance



Key: Know the contents of your code



Challenges In Technology Adoption & License Compliance





Why Do License Compliance?

- Code reuse is good engineering
 - OSS is used intentionally & unintentionally
- In most cases, there are no controls in place
 - Downloads bypass the purchasing department & management
 - Availability & quality of source makes re-use irresistible
- Licenses are assumed to be not applicable (e.g., AJAX) or unenforceable
- Crypto is assumed to be the correct rev or not there
- Less than honest reporting of OSS use
- Fear of delay caused by inefficient legal review





Why Do License Compliance?

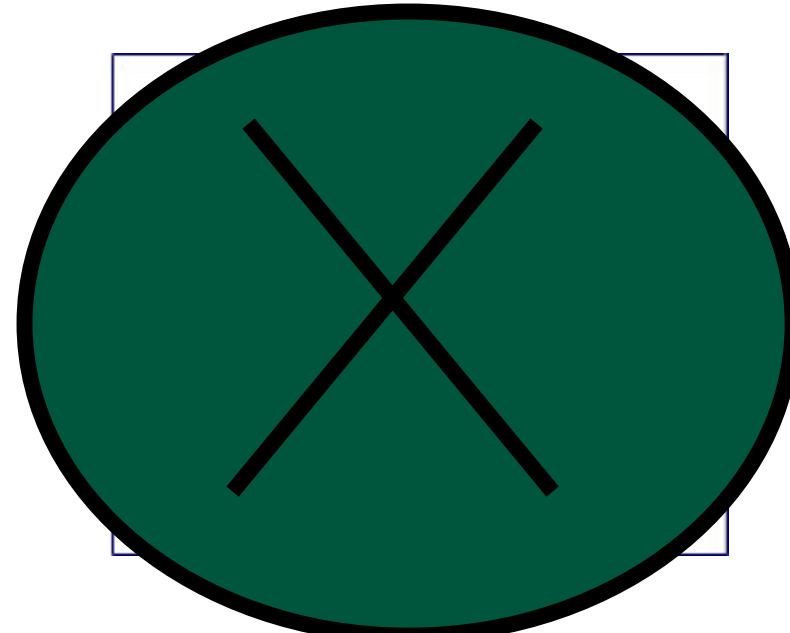
- Increasingly a standard part of the software development process
- Potential acquirers & investors know that automation decreases risks
- Portfolio companies facing special OSS due diligence by public companies in compliance frenzy
- Strategic partners want to know the contents of code
- Export Regulations
- End-users seek further assurances about code contents





Inadequate or No Compliance: Concerns

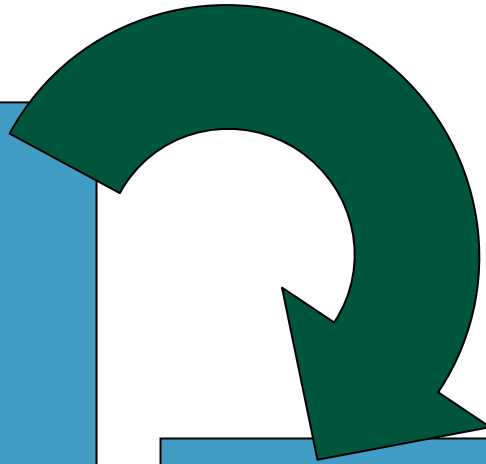
- Loss of IP rights
- Risk of IP infringement:
 - Automatic termination for violation of license
 - Required disclosure of source code
- Product export can be delayed or fines assessed
- Deal related impact: Lose, delay or reduce price on the deal
- Shareholder suits





Who's Involved in Compliance Today

- Developers
- Developer, QA, release & build management
- C-level & Boards of Directors
- Product managers & finance personnel
- Lawyers
- Third parties: Investors, I-Bankers, auditors, et al.



- At Funding
- Mergers & Acquisitions
- Partnerships & OEM deals
- Strategic Alliances & Product Resale
- Joint Development Projects
- Joint Ventures
- Product Export
- End Users



How To Start a Compliance Program



- It will involve:
 - Checklists
 - Executives & Developers
 - Code Analysis
 - Don't settle on a scan or string searches
 - Legal
 - Code remediation





10 Step Compliance Program

At the inception:

- (1) Form a core compliance team consisting of a
 - VP Engineering or senior engineering manager
 - Senior software architect or technology planner
 - IP or license attorney
 - Senior engineer
 - Senior release or QA manager may be helpful to help run the code analysis
- (2) Once formed, produce an operating charter
- (3) Create a timetable for the entire process

**Same as a
Due Diligence
Program**



10 Step Compliance Program



Before you do your code analysis:

(4) Prepare a list of software projects **and** licenses – past and present

(5) Identify any and all:

- Areas of potential or actual problem areas involving commercial, open source, third party or other code **and** licenses
- Projects which have a copy rights or patents filed by your company
- Open Source project Maintainers, and their acceptance policies
- development projects as “US-based” or “Offshore”
- Software suppliers of commercial, open source, third party or other code **and** licenses

**Similar to a
Due Diligence
Program**



10 Step Compliance Program



6. Do a Black Duck code analysis

- Use protexIP /Professional or /Enterprise – on premises solutions – or /OnDemand – a hosted solution.
- Using protexIP /OnDemand is often the best solution if you don't have a software compliance management solution in place.

7. Meet with the core compliance team

- Review the Black Duck code analysis final report

8. Present a plan consisting of:

- Of an explanation of the results of the code analysis report
- Remediation plan
- Timeline for remediation

9. Re-engage software development with recommendations & remediation plan

10. Repeat step #6

**Similar to a
Due Diligence
Program**



Compliance Program Results



Companies can ...

- Embrace more, or less, open source software
 - Sets proper tone re: compliance
 - Reduces time and cost of development
- Identifies issues early in development cycle
 - Reduce costs of remediation
- Efficiently engage legal counsel in code reviews
 - Gathers all available information automatically
- Track software IP & compliance through product lifecycle
 - From product concept through domestic or international product shipment



Black Duck provides software compliance management solutions that help companies govern how software assets are created, managed, and licensed

You need Black Duck...

- *If you build, buy, or sell software...*

or

- *If you audit, insure, or invest in companies with software...*



Thank You

*Leading Solutions for Software
Compliance Management*

