

Open Source Software: A Practical Approach to Governance in the Organisation

Balancing OSS Freedoms and Licence Responsibilities



Richard Kemp and Paul Garland, Kemp Little LLP

8 June 2010



Agenda

- Recent developments
 - Practice
 - Case law
- Practical approach to governance
 - The people context
 - OSS strategy
 - OSS policy
 - OSS processes
- The Client's view
 - With huge thanks to Tuli Day, Legal Director Business Units, SITA Legal
- 'OSS: Freedoms, Responsibilities and Governance' paper
 - in materials

OSS in the mainstream

- “Driven by a new pragmatism with its roots in creating software more efficiently and effectively, development organizations and companies are using open source to gain significant competitive advantage in a multi-source development process” (Black Duck CEO)
- “Just because something is free doesn’t mean it has no cost. Companies must have a policy for procuring OSS, deciding which applications will be supported by OSS and identifying the intellectual property risk or supportability risk associated with using OSS. Once a policy is in place, then there must be a governance process to enforce it” (Gartner Research Director)

Recent surveys

- Forrester (spring 09) ‘OSS Goes Mainstream’ report
 - OSS tops the IT issues list for decision makers inside the organisation
 - They want help to go “faster, cheaper, better”
 - OSS “hits on all these points”
- Black Duck (end 09) survey of 175 users
 - 20% of code base of average product or application is OSS
 - Cost of that OSS estimated at around \$25m per product/app
- Gartner (Nov 08) survey of 275 users worldwide
 - 85% of companies surveyed use OSS, remainder would do so in 12 months
 - 69% had no formal OSS policy
- Black Duck (spring 09) survey
 - Larger cos (>500 e’ees): 2 in 5 had formal OSS policy
 - SMEs (<500 e’ees): 1 in 5 had formal OSS policy

Current OSS licence top 20

Rank	Licence	%
1	GPL 2	48.46
2	LGPL 2.1	9.30
3	Artistic (Perl)	9.13
4	BSD 2.0	6.24
5	GPL 3	5.68
6	Apache 2.0	4.12
7	MIT	4.10
8	Code Project Open 1.02	3.07
9	Microsoft Public	1.58
10	Mozilla Public 1.1 (MPL 1.0)	1.22
11	Common Public (CPL)	0.55
12	Eclipse Public (EPL)	0.47
13	LGPL 3	0.45
14	zlib/libpng	0.43
15	Academic Free	0.40
16	CDDL	0.32
17	Open Software (OSL)	0.31
18	Mozilla Public 1.0 (MPL 1.0)	0.26
19	PHP 3	0.24
20	Ruby	0.23

- GPL (versions 2 and 3) accounts for over half the OSS world
 - Copyleft term
- The 4 FSF licences (GPL + LGPL, vs 2 and 3) account for 64%
- Academic licences (BSD, MIT) account for 10% - more liberal/permissive
- Top 4 licences account for 75%
- Top 10 licences account for 93%
- Trends:
 - No massive changes
 - GPL2 continues to be far and away the most used
 - GPL 3 is gaining popularity (adopted in Jun 07)

Cases – quick update

- Jacobsen v Katzer and Kamind – 19.2.10 settlement
 - OSS licence enforceable as a copyright licence not a contract (US CoA, .08.08)
 - Mr Jacobsen agreed to settle paying \$100k
- FSF v Cisco (.05.09 settlement) points the way for the future:
 - OSS compliance officer (OSCO) appointed + ongoing compliance reports
 - Publish code, compliant notices + monetary contribution to FSF
- Still no authoritative case law on key GPL issues:
 - What constitutes ‘distribution’
 - Extent of ‘copyleft’ in Article 2(b)
 - International aspects
 - Status of FAQs
 - Remedies
- ‘murmurings in the grasses’
- FSF’s objectives

Copyleft – quick reprise

- “2 You may modify your copy or copies of the Program or any portion of it, thus forming a **work based on the Program**, and copy and distribute such modifications or work ...provided that you also meet all of these conditions:
- b) You must cause any work that you **distribute** or publish, that in whole or in part **contains** or **is derived from** the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.”
- General consensus emerging on enforceability in principle
 - Much less consensus on how far enforceability extends
 - Just when does Program A (yours) **contain** or become **derived from** or **a work based** on Program B (the GPL code)?
 - The linking debate – static/dynamic link, system calls, plugs and sockets, etc
 - Just when is software **distributed**?
 - Debate centres on:
 - Classical (US) copyright law analytical techniques
 - FSF’s views (as expressed in FAQs, etc)
 - Emerging accepted software development practice in e.g. Linux and Java

The move to governance

- Tactical, ad hoc responses to OSS are (cost-)inefficient
- Traditional legal risk analysis is less effective:
 - Novel legal concepts
 - Absence of case law
 - Complexity of technical analysis
 - Way cases happen is different
- “Regardless of whether you view adoption of [OSS] as desirable or inevitable, the first step in moving from a tactical mess to a strategic plan is to specify the conditions under which [OSS] is permissible in your development shop. By creating a concise [OSS] policy, re-engineering the software acquisition process, and adding control points to [lifecycle management] processes and tools, application development professionals can shift from tactical responses to conscious integration based on realistic expectations and articulated economic benefits” (Forrester, spring 2009)

OSS governance is particular to each organisation

- No one size fits all
- Range of organisations and requirements – does your org:
 - only use OSS for internal purposes?
 - Public sector
 - Private sector
 - Use OSS in the products and services it markets?
 - Distribution
 - Hosted/ASP/SaaS use only

 - B2C organisation – OSS use more visible
 - B2B organisation
- Product spread:
 - E.g.. Device manufacturer of embedded software apps (mobile phones)
 - E.g. Fixed/mobile operator supplying services rather than products
- Geographical spread of operations

Governance: objectives and principles

Key objectives

- Similar to other IP-based policies and governance
- reducing/managing risk and maximising reward by:
 - **avoiding disputes** and managing regulatory risks;
 - achieving good management/housekeeping for a **financial event**
 - for example, an investment round, IPO or trade sale;
 - ensuring **customer satisfaction**; and
 - being a good **corporate citizen**.

Key principles

Key principles of OSS governance support these objectives:

- **acquisition**: know what OSS your organisation is using;
- **source reliability**: know where that OSS is coming from;
- **tracking**: know what that OSS does and where it is being used and re-used;
- **roles and responsibilities**: know who is responsible for what in relation to OSS; and
- **licence compliance**: know that your organisation is complying with its OSS licence obligations.

Governance: building blocks and threads

- Comprehensive, practical, analytical framework
- OSS achievements to date
 - The start point
- Thread 1: the people context
- Thread 2: the strategy context
- Thread 3: the policy context
- Thread 4: the process context

Thread 1: the people context

	STAKEHOLDER/GROUP	PRIME OSS OBJECTIVE	HOW OBJECTIVE IS ACHIEVED
1	CEO/Leadership Team	To manage and ensure effective use of OSS aligned with corporate strategy	Shaping and delivering best practice to achieve OSS governance
2	CFO/Finance Team	To identify, quantify and manage the organisation's OSS benefits and risks	Identifying and recording OSS components and licences and other commitments (such as other software assets)
3	CIO/Technical Team	To deliver OSS components and developments on time and on budget; to manage technical aspects of OSS governance programme	Implementing technical side of OSS governance (e.g. code indicator tool)
4	Customers	To gain business advantage through use of the organisation's technology/services in knowledge that OSS risk is being managed	Performing contractual commitments contained in contracts with the organisation
5	Developers	To know that OSS use is encouraged and to understand how he/she is able to use OSS in daily work	Following OSS governance and feeding back on possibilities for improvement
6	Directors/Supervisory Board	To ensure that the organisation adopts appropriate OSS governance aligned to organisation's strategy	Formulating effective OSS governance policies and ensuring they are properly implemented
7	OSS Compliance Officer ('OSSCO')	To develop and implement OSS governance and ensure ongoing compliance with it	Articulating, agreeing and implementing OSS strategy, policy and process statements
8	OSS Working Party ('OSSWP')	To provide a focal point for interests of organisation's stakeholders and a crucible for OSS governance	Managing OSSCO; communicating back to other stakeholders
9	HR Team	To understand the HR and legal status to be given to OSS governance and policy statements	Ensuring that OSS policy statement forms part of the organisation's employee/contractor handbook
10	Legal Team	To minimise legal risks and maximise benefits to the organisation in its contractual commitments and OSS governance	Helping other stakeholders to manage OSS governance, with particular emphasis on documents (statements, contracts and so on)
11	Sales & Marketing Team	To generate revenue generation & reduce cost while ensuring customer satisfaction	Preventing unauthorised OSS use
12	Shareholders	To maximise share value	Using OSS in an efficient, compliant way to achieve cost reduction, increase in profit, increased competitiveness, increased efficiencies and reduced IP leakage
13	Suppliers	To perform contractual commitments in contracts with the organisation	Compliance with the organisation's inbound transactions/procurement policies for OSS

Thread 2: the strategy context

OSS STRATEGY STATEMENT FOR [ORGANISATION]

- [Organisation]'s OSS objectives.** [Organisation] will continue to use OSS in order to increase [Organisation]'s:
 - ability to attract the best talent by building a development community at the forefront of OSS skills;
 - competitiveness by increasing development and operational efficiency and effectiveness, enabling faster time to market and reducing costs; and
 - value to stakeholders.
- OSS compliance.** [Organisation] fully recognises and respects the rights of, and its agreements with, others just as it expects others to respect [Organisation]'s rights and perform their agreements with us. Accordingly, [Organisation] respects the need to ensure compliance with its legal obligations in licence agreements for OSS that it uses.
- OSS governance within [Organisation]: achieving the right balance.** [Organisation] is committed to implementing best-practice OSS governance. The purpose of [Organisation]'s best-practice OSS governance is effectively, appropriately, proportionately and transparently to balance the objectives set out at paragraph 1 and the compliance expectation set out paragraph 2. This balance will be achieved:
within [Organisation]:
 - by supporting [Organisation]'s development community in its work - as governance for developers by developers;
 - by effective communication, including educating, training and raising/maintaining awareness of OSS issues among all stakeholders;
 - by taking into account the interests of all stakeholders; and
 - through the active and timely support of all stakeholders;***with [Organisation]'s partners:***
 - by ensuring that [Organisation]'s supplier and customer partners are aware of and comply with their OSS obligations, through [Organisation]'s contracts and appropriate relationship management.
- The mixed software environment.** [Organisation]'s use of OSS will continue to be in a 'mixed' software environment:
 - using OSS and proprietary software owned by [Organisation] and third parties;
 - constantly evaluating where OSS is best used within [Organisation]; and
 - re-using OSS components where appropriate thereby leveraging [Organisation]'s knowledge and technical resources.
- Further details.** This strategy statement forms part of [Organisation]'s OSS governance along with our policy statement and process statement. It is subject to review and change. For further details please contact [Organisation]'s OSS Compliance Officer at [email] and our OSS online resource kit at [intranet URL].

Thread 3: the policy context

A. Scope and rationale

- Purpose
- Who does it apply to?
- What's its status
- Authorisation process
- Mixed licensing model – proprietary, academic and reciprocal models
- Statement that Org will comply fully with all software licences, irrespective of type

B. Roles, responsibilities, training & awareness

- OSSCO as developers' first line of support
- OSS Working Party (OSWP)
 - oversight of OSSCO
 - members drawn from stakeholders (+ legal)
- Training and awareness
 - Regular, frequent training by OSSCO/WP
 - To ensure strategy and policy are understood and met

C. Policy for:

- Inbound transactions
 - Pre-contract: approach to RFIs, etc
 - Approach in procurement contracts
 - Statement about warranty/indemnity/remediation
 - Inbound development agreements
 - M&A
- Inhouse development
 - Authorisation mechanism
 - Pre-approved OSS s/w, OSS licences
 - Code assessment through indicator tool
 - OSS licence approval and guidance process
- Contributions to OSS projects
- Outbound transactions
 - Template licence/services agreements enshrine approach
 - Approval levels
 - Involvement of Legal

Thread 4: the process context

A. Dependencies on/links with:

- OSS strategy and policy statements
- Patents/other IP policies
- Groups overseeing product architecture and strategic direction
- Source code management
- HR policies
- Inbound/outbound contract groups

B. Pre-implementation

- Planning, mapping and timing:
 - treat like any other major development project
- Indicator tool procurement and implementation
- Initial code assessment
- Consider amnesty
- Consider pilot project implementation

C. Implementation

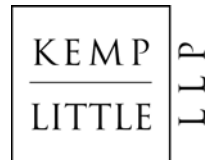
- Approval for 'top X' licence
 - Accessible 'do's' and 'don'ts'
 - White lists:
 - Intranet URL for OSS components approve
 - Intranet URL to show OSS licences approved
 - Black list
 - List s/w, licences barred or requiring prior approval
- Pre-launch/release compliance
- OSSCO, OSSWP service levels]

D. Post-Implementation

- Code/information repository
- Periodical code assessment
- Remediation arrangements
- Training and awareness

The Client's view - SITA

- *With huge thanks to Tuli Day, Legal Director Business Units, SITA Legal*
- The world's leading specialist in air transport communications and IT solutions
- Delivering and managing business solutions for airline, airport, GDS and other customers over the world's most extensive network which forms the communications backbone of the global air transport industry
- 550 air transport industry members
 - Over 90% of the total worldwide airline business
- 3,200 customers in over 200 countries
- 4,500 employees from over 140 nationalities speaking over 70 different languages
- \$1.5bn of revenues



The client's view: governance take-aways

1. Buy-in of key stakeholders is essential
 - even then implementation costs hard to overcome
2. Main concepts communicated to decision makers:
 - "governance process for developers by developers"
 - governance allows you to "understand your code base"
 - "only the unmanaged use of open source is a risk"
3. Pilot
 - Approach was to do a pilot to ease fears of cost increases due to remedial action.
4. Awareness raising proved not to be as useful as commonly thought when wanting to implement governance
 - created more FUD rather than hard evidence of what was in the code base
5. What was more useful was freeing up developer time with knowledgeable use of open source
 - mainly through guidance on specific licences
 - so they went for it for the positives rather than the negatives
6. Internal risk assessment was carried out by corporate risk
 - to ensure that the open source risk was in the corporate risk governance model.
7. Legal Dept involvement:
 - Legal sits on corporate OSS steering group.
 - approach was to provide tools and awareness to key users in the development team to equip them to handle the broad ranging issues
 - dev team only comes to legal with eg new licences - ie success was owned by development as well as legal.
 - All requests from development go to the steering group to get consistency of approach.
8. Future still involves making sure open source governance remains a benefit rather than a burden
 - so training is being targeted
 - as is raising the company's profile as a good user of OSS in its customer communications etc

Questions?

Richard Kemp

Senior Partner

Kemp Little LLP

richard.kemp@kemplittle.com

Tel. +44 (0) 20 7710 1610



Paul Garland

Head of Litigation

Kemp Little LLP

paul.garland@kemplittle.com

Tel. +44 (0) 20 7710 1617

