

## OPEN SOURCE SOFTWARE (OSS) GOVERNANCE IN THE ORGANISATION

### A. INTRODUCTION

**Recent surveys.** When IT consultancy Gartner released its survey in November 2008 of OSS use by 274 end user organisations around the world, it came up with two key findings:

- At that time, 85% of the companies surveyed used OSS, and the remaining 15% were expecting to do so within the next 12 months.
- 69% of the companies surveyed had no formal policy for evaluating or cataloguing use of OSS within their organisation.

As in the aftermath of the dotcom bust, continuing tougher economic times are hastening the uptake of OSS within organisations which, according to Gartner's statistics, now approaches ubiquity. However, by all accounts there is still a disconnect between uptake and effective governance: on Gartner's figures, OSS governance remains more widely honoured in the breach than the observance. In the press release that accompanied its November 2008 survey, Gartner's research director Laurie Worster said:

**“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”<sup>1</sup>.**

Gartner's findings were corroborated by a survey published in March 2009 by Black Duck Software<sup>2</sup>, which (although of a smaller survey sample) found that only 40% of larger companies (those which employed 500 developers or more) had written governance policies and, of the sample as a whole including SMEs, only one in five had written governance in place.

**Purpose.** OSS governance is now, somewhat belatedly, rising up the corporate agenda<sup>3</sup> and the purpose of this article is to suggest a practical approach to creating documentation which will implement sensible, proportionate OSS governance<sup>4</sup>. This approach is based on the premise that most organisations wish for

---

<sup>1</sup> <http://www.gartner.com/it/page.jsp?id=801412> - Gartner press release of 17 November 2008: “Gartner Says as Number of Business Processes Using Open-Source Software Increases, Companies Must Adopt and Enforce an OSS Policy”.

<sup>2</sup> <http://www.blackducksoftware.com/news/releases/2009-03-11> - Black Duck press release of 11 March 2009: “Black Duck Survey Reveals Open Source Development Trends”.

<sup>3</sup> See e.g. the abstract from IT research company Forrester's paper “Best Practices: Improve Development Effectiveness Through Strategic Adoption Of Open Source” of 2 February 2009: “[OSS] is getting renewed attention from application development professionals who are looking for cost-saving alternatives amid the economic recession. But many aren't asking the right question: Instead of “should we adopt [OSS]?” they should be asking, “how will we adopt [OSS]?” [OSS] is already seeping into development shops through a variety of channels, whether managers know it or not. Unchecked tactical adoption of [OSS] creates unmanaged risk and unrealized returns, and application development professionals should not tolerate it. 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” (<http://www.forrester.com/Research/Document/Excerpt/0,7211,46361,00.html>).

<sup>4</sup> With the historically low take up of more formal OSS governance there has until recently been relatively little publicly available online material about OSS governance. OSS software/support developers Black Duck, Palamida and HP's FOSS Bazaar provide resources at:

- <http://www.blackducksoftware.com/resources/whitepapers#managingos> (Black Duck);
- [http://www.palamida.com/themes/resources/Palamida\\_WhitePaper\\_PCIComplianceAtRisk.pdf](http://www.palamida.com/themes/resources/Palamida_WhitePaper_PCIComplianceAtRisk.pdf) (Palamida);
- <https://fossbazaar.org/openSourceGovernanceFundamentals> (White paper on FOSS Governance Fundamentals) and <https://fossbazaar.org/content/best-practices-open-source-governance> (Best Practices in Open Source Governance).

reputational and competitive reasons to be seen to be good corporate citizens in their use of OSS. We propose a three-tier approach which ensures that internal governance discussions result in staff throughout the organisation buying into its statements of strategy, policy and process, and integrating them fully with how the organisation works. There is no magic to this approach, which focuses clearly on the high level issues, the policy that the organisation will define for its stakeholders and the day-to-day processes around implementation: collectively the OSS governance toolkit.

**Scope.** Different organisations' circumstances will differ widely so it is not practical to offer template 'one-size-fits-all' documents. However, this article offers pointers as to what stakeholders should consider when developing OSS governance for their organisation and the areas that should be covered by strategy, policy and process statements.

Although the purpose of effective OSS governance is to establish a practical, event-driven mechanism which enables an organisation to make good decisions on the range of particular questions that arise, this article does not itself address any of the granular technical OSS issues that continue to absorb significant amounts of management, technical and legal time, such as:

- the multiplicity of OSS licences;
- the 'do's and don'ts' for licences and licence families themselves;
- GPL-related issues as to what constitutes 'distribution'; and
- 'copyleft' – GPL-related questions of software derivation and combination associated particularly with use of the Java platform and the Linux platform<sup>5</sup>.

## **B. FUNDAMENTALS OF OSS GOVERNANCE**

**Objectives.** Embarking on the journey towards effective OSS governance can be a challenging process for any organisation. Starting out, it is critical to know the direction of travel: what are the organisation's objectives for OSS and governance? As with other intellectual-property-based policies and governance, these can generally be succinctly stated in terms of reducing/managing risk and maximising reward by:

- (i) avoiding disputes and managing regulatory risks;
- (ii) achieving good management/housekeeping for a financial event – for example, an investment round, IPO or trade sale;
- (iii) ensuring customer satisfaction; and
- (iv) being a good corporate citizen.

**Key principles.** Supporting these objectives, the key principles of OSS governance may similarly be concisely articulated as:

---

See also the OLEX (OpenLogic Exchange) Wazi at <http://olex.openlogic.com/wazi/2009/create-open-source-policy/> (Best Practices for Creating an Open Source Policy) and <http://olex.openlogic.com/wazi/2009/create-an-open-source-governance-process/> (From Policy to Process: Best Practices for Creating an Open Source Governance Process); and <http://www.softwarefreedom.org/resources/2008/foss-primer.pdf> (a Legal Issues Primer for Open Source and Free Software Projects). In the published books, see in particular Meeker, *The Open Source Alternative*, Wiley, 2008, Chapters 10 (Developing a Corporate Open Source Policy) and 10A (Open Source Corporate Policy) and Woods/Guliani, *Open Source for the Enterprise*, O'Reilly, 2005, Chapter 7 (Designing an Open Source Strategy).

<sup>5</sup> For further information, see the Kemp Little paper 'Open Source Software: an Introduction' (July 2009 edition) [http://www.kemplittle.com/PDFs/Article\\_IntroductionToOpenSource.pdf](http://www.kemplittle.com/PDFs/Article_IntroductionToOpenSource.pdf)

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

**OSS governance is particular to each organisation.** Effective OSS governance does not operate in a vacuum. It is relatively simple to state the basic key OSS governance objectives and principles, but applying them to a specific organisation requires that they be tailored, both in terms of high-level strategy and tactics, and day-to-day operational procedure.

**The range of organisations for which OSS governance is relevant.** If your organisation only uses OSS for internal purposes – that is, there is no re-distribution outside the organisation – the issues (and therefore the governance) will differ from those of an organisation that uses OSS in the products or services that it markets. Equally, in the ‘internal use only’ case, the position of a public sector organisation – say a Government Department or Local Authority - will be different from the private sector as public sector organisations, in their drive to use public money wisely, may be encouraged or mandated to use OSS over proprietary solutions and may have more formal, even statutorily prescribed, procurement procedures which OSS governance will need to be consistent with.

If your organisation develops software using OSS and then distributes software with OSS components (whether as a service or as a licence), the issues arising will probably be different and more complex issues than those involved where the use is only internal. There will also be a difference in emphasis depending on whether you are a business-to-consumer (‘B2C’) organisation supplying OSS components contained in the software you sell, or a business-to-business (‘B2B’) organisation whose end-user customers are other organisations who then sell on to the consumer. Other factors affecting the emphasis that OSS governance will take in any particular case include:

- The geographical spread of the business(es) – a company with a number of development centres around the world will look at things differently from a company with all its developers under one roof.
- Product spread – to take an example from the communications industry, a manufacturer of devices with embedded software applications like mobile phones will be in a different position from a fixed or mobile operator who principally supplies telecoms services rather than products (even if, as in the case of BT, the service may be delivered using a router containing embedded OSS applications as part of the service).

**Contexts of OSS governance – building blocks, threads and integration.** It is helpful to think of the components of successful OSS governance as building blocks, linked or threaded together by context. These connecting start with ‘achievements to date’ and previous experience of OSS governance implementation; they then integrate the people context (Section C, Table 1 below); the strategic context (Section D, Table 2); the policy context (Section E, Table 3); and the process context (Section F, Table 4). Each thread, and the individual building blocks in it, need then to be integrated across the organisation to set the context.

**OSS achievements to date.** Each organisation at the stage where it is considering formalising OSS governance will almost certainly have arrived at a start point which likely has some notable OSS achievements to date – it might have shaped the core OSS issues it faces in its business and may already have done ad hoc work identifying the top OSS licences it uses.

**C. THREAD 1: THE PEOPLE CONTEXT**

OSS use in the organisation on anything other than a purely ad hoc basis will involve a number of stakeholder groups both inside and outside the organisation, and effective OSS governance will depend on them integrating and cooperating in a way that is supportive and positive. There may well be many interested stakeholders whose interests will need intermediation in order to arrive at an agreed approach to governance. In Table 1 below, we have shown by way of illustration a description of potential stakeholders in an organisation, their possible objectives in relation to OSS and how those objectives can be achieved.

**TABLE 1 - STAKEHOLDERS, THEIR OSS OBJECTIVES AND HOW THEY ARE ACHIEVED**

<b>STAKEHOLDER/GROUP</b>	<b>PRIME OSS OBJECTIVE</b>	<b>HOW OBJECTIVE IS ACHIEVED</b>
<b>1 CEO/Leadership Team</b>	To manage and ensure effective use of OSS aligned with corporate strategy	Shaping and delivering best practice to achieve OSS governance
<b>2 CFO/Finance Team</b>	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)
<b>3 CIO/Technical Team</b>	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)
<b>4 Customers</b>	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
<b>5 Developers</b>	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
<b>6 Directors/Supervisory Board</b>	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
<b>7 OSS Compliance Officer ('OSSCO')</b>	To develop and implement OSS governance and ensure ongoing compliance with it	Articulating, agreeing and implementing OSS strategy, policy and process statements
<b>8 OSS Working Party ('OSSWP')</b>	To provide a focal point for interests of organisation's stakeholders and a crucible for OSS governance	Managing OSSCO; communicating back to other stakeholders
<b>9 HR Team</b>	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
<b>10 Legal Team</b>	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)
<b>11 Sales &amp; Marketing Team</b>	To generate revenue generation & reduce cost while ensuring customer satisfaction	Preventing unauthorised OSS use
<b>12 Shareholders</b>	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
<b>13 Suppliers</b>	To perform contractual commitments in contracts with the organisation	Compliance with the organisation's inbound transactions/procurement policies for OSS

## D. THREAD 2 – THE STRATEGY CONTEXT

OSS governance does not operate in a vacuum. At the highest level, it should align with other statements of organisational strategy – including corporate, risk management and IP strategy generally. The OSS strategy statement is also the mechanism by which stakeholders can establish and express an internal consensus. It can then provide a key point of reference for communication and education and for the development of the OSS policy statement. The organisation’s leadership must be able to intermediate between the different groups and arrive at an agreed, short, clear, high-level statement about where and why it will and will not use OSS. Each particular organisation adopting OSS Governance will need to consider its approach, but a suggested illustrative OSS strategy statement is set out at Table 2 below.

**TABLE 2 - OSS STRATEGY STATEMENT FOR [ORGANISATION]**

1. **[Organisation]’s OSS objectives.** [Organisation] will continue to use OSS in order to increase [Organisation]’s:
  - o ability to attract the best talent by building a development community at the forefront of OSS skills;
  - o competitiveness by increasing development and operational efficiency and effectiveness, enabling faster time to market and reducing costs; and
  - o value to stakeholders.
2. **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.
3. **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]:***
    - o by supporting [Organisation]’s development community in its work - as governance for developers by developers;
    - o by effective communication, including educating, training and raising/maintaining awareness of OSS issues among all stakeholders;
    - o by taking into account the interests of all stakeholders; and
    - o through the active and timely support of all stakeholders;
  - with [Organisation]’s partners:***
    - o 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.
4. **The mixed software environment.** [Organisation]’s use of OSS will continue to be in a ‘mixed’ software environment:
  - o using OSS and proprietary software owned by [Organisation] and third parties;
  - o constantly evaluating where OSS is best used within [Organisation]; and
  - o re-using OSS components where appropriate thereby leveraging [Organisation]’s knowledge and technical resources.
5. **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].

## E. THREAD 3: THE POLICY CONTEXT

The heart of OSS governance is the OSS policy statement. A well-crafted policy should:

- Be *clear and brief*, otherwise people won't read and understand it.
- Be *event-driven*, setting out roles and responsibilities: to whom should OSS queries be addressed, and who does what in particular scenarios?
- Set out *criteria and decision points* for OSS use. Apply Occam's razor – the simplest answer is usually the best – and try to calibrate the policy so it will settle 80% of decisions, while also providing for effective management of exceptions.
- Set out the *information* to be collected and tracked.

Although, again, each organisations will need to consider what is appropriate for its own circumstances, we have also suggested illustrative wording for an OSS policy in Table 3 below around three main headings: scope and rationale; roles, responsibilities, training and awareness; and transaction type (inbound, in-house and outbound). The wording gives a starting point which will need to be adapted to fit the circumstances of the particular organisation involved.

**TABLE 3 - OSS POLICY STATEMENT FOR [ORGANISATION]**

### A. SCOPE AND RATIONALE

#### 1. **Scope**

- **Purpose:** This policy statement is designed to supplement our existing policy and processes relating to [Organisation]'s products and services. It deals specifically with those development and licensing considerations which must be fully understood and complied with when using and otherwise dealing with OSS within products and services that [Organisation] [markets][uses].
- **To whom does this policy statement apply?** This policy statement is mandatory and applies to everybody in [Organisation] who is responsible for [product design, launch and support] across all [Organisation]'s solutions, whether as an employee or contractor. The intention is to ensure that [Organisation] fully understands and complies with the obligations and duties as contained in the relevant OSS licence terms, and is also seen to do so.
- **What is the legal status of this policy statement?**<sup>6</sup> This policy statement [forms part of [Organisation]'s HR handbook (for employees) and part of the Contractor handbook (for corporate and individual contractors)] and

<sup>6</sup> A number of related issues arise here.

First, the HR aspects of the Policy are particularly important in considering how the organisation will ensure that OSS governance is effective. If it already has IT (email acceptable use for example) or intellectual property policies that are incorporated expressly or by reference into the HR handbook or even the contract of employment, it will be relatively straightforward to treat OSS governance similarly. If there is nothing comparable already in place, a number of questions need to be addressed, including particularly consequences of non-compliance where a developer uses OSS otherwise than in accordance with the OSS Policy or contributes to a OSS project otherwise than as permitted.

Secondly, how 'binding' does the Organisation want the policy statement to be on staff and/or contractors? If it is not of any binding effect, the policy may lack teeth. If it is binding, the usual way is to follow the language at the end of this bullet, and to say it forms part of the engagement arrangements. Either way, it should be consistent with policy statements that may be regarded as equivalent, like email acceptable use or IP policies for example.

Thirdly, HR difficulties can be compounded by the tension that generally arises between copyright law (where copyright in software developed by an employee in the course of his or her employment generally vests in the employer by operation of law) and code contributions to OSS projects (which generally provide that copyright in code contributed to the project is owned by the project). Again, corporate policy needs to be thought through and articulated in advance here.

Fourthly, it is worth remembering that under English law for example software developed by a contractor – whether an individual or a corporation – needs to be expressly assigned in order to belong to the organisation engaging the contractor.

accordingly has the same legal status as equivalent policy statements – [that is to say, it [forms part of your engagement terms with the Organisation]];

- o **Design process:** All products and services that [Organisation] markets and that contain OSS must be [design-approved by the [Organisation] [review body OR OTHER AUTHORISED BODY OR PROCESS], taking into account architectural, security, legal, commercial and all other relevant considerations. In particular, as part of that design approval OSS licence terms must be understood and processes put in place to ensure [Organisation] compliance once the product/service is launched.
- o **Code indicator tool<sup>7</sup>:** All source code in products and services that [Organisation] markets are to be scanned before launch using an OSS indicator tool. This will enable OSS code to be identified and all associated OSS licences to be checked for compliance with the licence's terms. Information from the scan must be acted on so as to ensure [Organisation]'s compliance with the obligations in the relevant OSS licences.
- o **Further details:** This policy statement forms part of [Organisation]'s OSS governance along with our strategy statement and process statement. It is subject to review and change. For further details please contact [Organisation]'s OSS Compliance Officer at [email] and see our OSS online resource kit at [intranet URL].

## 2. **Rationale**

- o The rationale behind this part of the policy statement is to provide an introduction to OSS models and ensure OSS licences are given the attention and respect they require as a legal document.

The licensing of OSS code follows a different style of business model to the type [Organisation] has historically been used to. Most proprietary software is licensed under what can be called a *proprietary model*, where the copyright owner reserves all the rights the law grants, except for certain specific rights which are granted for a licence fee (for example, for £10 I license you (grant you permission) to use, but not to copy, modify or publish etc the software). OSS code on the other hand is in the main licensed either under:

- an **Academic Model** - such as the BSD, MIT, AFL or Apache licenses. Academic OSS Licences are typically light-touch agreements that basically seek “Freedom” for the software code. The main positive obligation on the Licensee is the duty to identify the origins of the OSS code – “attribution” ; or
- a **Reciprocal Model** - such as the GPL, MPL, CPL and EPL. Reciprocal OSS Licences are generally more assertive in putting positive obligations on the Licensee with the objective of ensuring that all the copyright owner's rights (to use, copy, modify, publish and so on) are passed down to other users.
- o [Organisation] will continue to operate in a ‘mixed’ software environment, using proprietary software under the *proprietary model* and (for OSS) the *Academic model* and the *reciprocal model*.
- o Regardless of the underlying model, every software licence that attaches to software code (whether proprietary or OSS) constitutes a legal agreement between the licensor and the licensee. [Organisation] will comply fully with its legal obligations as set out in any licence agreement attaching to software code that is used within [Organisation], including that used within [Organisation] products or services.

## **B. ROLES, RESPONSIBILITIES, TRAINING AND AWARENESS**

### 3. **Roles and responsibilities**

- o **OSS Compliance Officer<sup>8</sup>:** In order to help [Organisation] achieve its OSS objectives, [Organisation] has created the position of OSS Compliance Officer (‘OSSCO’). OSSCO will be the first line of support for the development community within [Organisation] on questions you may have about OSS.
- o **OSS working party<sup>9</sup>:** OSSCO will report to the OSS working party (‘OSSWP’). The OSSWP has members drawn from [Organisation]'s stakeholders. The role of the OSSWP is to give guidance to the OSSCO and,

<sup>7</sup> The products of specialist OSS service providers like Black Duck, Palamida and Fossology and the code indicator tools and other technology platforms they supply can automate and take significant cost out of manual processes. An OSS indicator tool in particular serves a number of purposes. First, the code base of the organisation can be run through the tool in order to assess what OSS is currently in use internally; output in some cases can be aligned with the organisation's source code management system. Secondly, on an inbound transaction, the organisation can use the tool to assess what OSS is in use, e.g. in an acquisition target (and check that the responses to due diligence for example are complete and accurate), or where the company is licensing in software from a third party. Thirdly, a number of the commercially available indicator tools can be ‘parameterised’/programmed in advance to set up agreed ‘do’s’ and ‘don’ts’ – rule of the road – for in-house OSS use. See also Table 4, Part B below (Processes).

<sup>8</sup> The OSSCO and the OSSWP are the lynchpins of the OSS governance process. The OSSCO is generally drawn from the development or technical rather than Legal team in practice, with Legal team representation on the working party.

<sup>9</sup> See previous footnote.

reporting to [ ], to ensure that [Organisation]'s use of OSS is aligned with [Organisation]'s strategy and the OSS strategy statement.

4. **Training and awareness**<sup>10</sup>. OSSCO and the OSSWP will organise and carry out regular and frequent OSS training and awareness to ensure that the principles of [Organisation]'s OSS strategy and policy are understood and met throughout [Organisation].

**C. OSS POLICY FOR INBOUND TRANSACTIONS, IN-HOUSE DEVELOPMENT AND OUTBOUND TRANSACTIONS**<sup>11</sup>

**5. OSS policy for inbound transactions**

o *OSS in [Organisation]'s procurement policies*

- Pre-contractual documents (RFIs, RFPs, and so on) and contracts are to provide that software deliverables to [Organisation] will not contain OSS unless OSS components have been individually identified before contract signature and expressly agreed by [Organisation].
- [Organisation]'s procurement contracts will reserve the right for [Organisation] to apply code indicator tool to carry out assessment in any case.
- [Organisation]'s procurement contracts will include warranty/indemnity protection for non-identified/agreed OSS and (in addition to normal remedies) provide for rewriting as remediation on case-by-case basis.

o *OSS in inbound development agreements:* as per procurement policies outlined above.

o *OSS in M&A:*

- Technical and legal due diligence to be configured to enable all OSS in target company's code base to be identified early on.
- Consider using code indicator tool provider on escrow basis to carry out independent assessment.
- Allow sufficient time between signature of contracts and closing/completion for remediation by rewriting.

o OSSCO and [legal representative of [Organisation]] will be available to discuss particular issues arising on inbound transactions.

**6. OSS policy on in-house development**

o *outline of authorisation mechanism:*

- OSG will operate across the organisation on the basis of pre-approved OSS components/software and the OSS licences that attach to them.
- Assessments through indicator tool: [Organisation] will:
  - assess what OSS it [and its contractors] are using in its operations; and
  - associate the relevant OSS licences with the OSS so assessed to be used;by:
  - assessing 'incoming' code using the code indicator tool;
  - pre-launch/release code assessments; and
  - carrying out periodical assessments of internally developed code to verify that the OSS being used within [Organisation] is what is expected to be used;
- Remediation where necessary: Co will develop a process to review, assess and remediate instances of non-compliance with [Organisation]'s policy statement or otherwise in relation to a particular OSS licence;

o *OSS licence approval*

- approval will be on the basis of the OSS licences determined to be most commonly used within [Organisation];
- *Approval 'do's and don'ts':* approval will be to enable use of the software concerned on the basis of clear, short, simple 'do's and don'ts' addressing the needs of Co developers;
- *Scope of approval:* Unapproved open source software, software licensed on an unapproved licence, or use outside the 'do's and don'ts' will be prohibited;

<sup>10</sup> An effective, continuing communication, training and awareness programme is of the essence of good OSS governance.

<sup>11</sup> The OSS policy should be event driven – i.e. it needs to think through and define in advance the sorts of issues that will arise. It should then aim to prescribe decision making which will deal with 80% of the issues that arise, with effective escalation to deal promptly with the other 20%. The events in this illustration are defined by reference to inbound, in-house and outbound transactions.

- *Post-implementation approval*: The post-implementation approval process will involve the OSSCO and will be designed to support the development community in giving timely positive assistance whilst respecting open source licence obligations;
7. **[Organisation]’s policy on contributions to OSS projects.** [set out here whether and if so to what OSS projects and on what terms [Organisation] developers may contribute code and other work<sup>12</sup>.
  8. **OSS policy on outbound transactions.**
    - o [Organisation]’s template [licence/services agreements] set out [Organisation]’s approach to OSS in its customer contracts;
    - o OSSCO and [legal representative of [Organisation]] will be available to discuss particular issues arising on outbound transactions.

## F. **THREAD 4: THE PROCESS CONTEXT**

The OSS processes should take the strain of OSS governance. The process context is where the interrelationships with and *dependencies* (Section A of Table 4 below) on policies outside the OSS area and other building blocks and threads within it need to integrate. The *pre-implementation* steps that the organisation may need to take are set out at Section B of Table 4. The project should be *implemented* like any other development in the organisation, with proper resource allocation, planning, mapping and timetabling (Section C of Table 4). Consider using a pilot in one part of the business to gain experience that can then be rolled out across the organisation as a whole. Consider also an amnesty to get the development community onside – winning hearts and minds. As a practical matter, the importance of technology platforms to minimise time and cost, increase efficiency, enhance collaboration, improve record-keeping and ensure validation can scarcely be over-emphasised. The OSS governance processes will need to be supple enough to cater for the full range of activities *post-implementation* (Section D of Table 4).

**TABLE 4 - CHECKLIST FOR OSS PROCESS STATEMENT FOR [ORGANISATION]**

### **A. DEPENDENCIES**

#### **1. Dependencies on/links with:**

- o OSS governance strategy and policy statements;
- o [Organisation] patents and other IPR policies;
- o Relevant stakeholder groups such as the group(s) within the Organisation responsible for software architecting and strategic direction;
- o Source code management (including tools such as concurrent versions systems (CVS) and subversion);
- o HR policies;
- o Inbound/outbound contract groups;
- o Exit strategy (if applicable).

### **B. PRE-IMPLEMENTATION**

2. **Project planning, road mapping, timetabling.** Treat implementation of OSS governance at the process level like any other development project – with sufficient/appropriate resources, and detailed project planning, road mapping, dependency management and timetabling.
3. **Indicator tool implementation<sup>13</sup>.** Consider procurement of, and budget implications for, indicator tool well in advance of OSS governance implementation.
4. **Initial assessment.** Consider initial code assessment (NB: make sure you can continue to use the assessment results even after the contract with the indicator tool provider has terminated).

<sup>12</sup> See footnote 8.

<sup>13</sup> See also footnote 7 above.

5. Consider **amnesty** for developers pre-implementation to encourage/bolster need for compliance use post-implementation.
6. Consider **pilot project** implementation initially before roll out across [Organisation].

### **C. IMPLEMENTATION**

7. **Approval for OSS licences most commonly used.**
  - o Identify [Organisation]'s 'top [X]' OSS licences most commonly used within [Organisation], e.g.: [list];
  - o Refer to [intranet hyperlink] for methodology of how these OSS licences have been identified and analysis;
8. **Approval 'do's and don'ts'**
  - o Consider approval on the basis of short form, easily accessible/readable '*Do's and Don'ts*'.
  - o Consider maintaining intranet URL to show OSS [components] whose licences have been approved.
  - o Consider maintaining separate intranet URL to show OSS licences that are approved for use.
  - o Consider maintaining separate intranet URL of OSS components/licences (if any) whose use always requires prior specific approval from FOSSCO/legal.
9. **Pre-launch/release compliance** check using code indicator tool or otherwise.
10. Set out **service levels** for FOSSCO/FOSSWG responses to individual questions outside scope of policy/process guidance.

### **D. POST-IMPLEMENTATION**

11. Arrangements for **code and other information repository**.
12. Periodical **code assessment**.
13. **Remediation** where necessary.
14. **Training and awareness**.

## **G. CONCLUSION**

As OSS use in the organisation approaches ubiquity, OSS governance is rapidly becoming a 'must have' not just a 'nice to have' in order to manage risk and benefit effectively. Each organisation's needs will be different, and senior management will need to consider all aspects of this complex question carefully before embarking on OSS governance implementation, as they would any sophisticated software development project. At the end of the journey, management is looking to have in place integrated processes across all relevant business functions to manage effective use of OSS throughout the organisation. To get there, it should consider disassembling the various pieces into their building block components and threading them together by start point (achievements to date), people (stakeholders) and the strategic, policy and process aspects.

**Kemp Little LLP (RHK), December 2009**