

# **Open Source Governance for your Organization**

## Before we get started

- Per my website:

*The content on this site is my own and does not necessarily represent my employer's positions, strategies or opinions.*

- <http://www.sutor.com>
- This discussion does not constitute legal advice.
- I'm not an attorney, and certainly not an intellectual property attorney, and you should consult one as necessary.

# The key question

Do you have proper legal controls and business processes in place to deal with open source software?

## Your open source governance strategy

- Five years ago, it was not uncommon for that strategy to be defined as “you shall use no open source software.”
- You need to understand the legal risks and responsibilities for any software you use, and weigh those against the business value.
- Work out a plan that specifies what business and legal controls are in place to approve use of open source in your organization or in your products, and make sure you have a well defined escalation path.

## What you need to know

- All projects to which your employees or organizational members contribute, the free and open source licenses being used, and the intellectual property commitments those contributions make upon your company or organization.
- All use of open source code within internal processes, product development, and services engagements.

## What you need to know

- All open source code that goes into your hardware products, software products, web-delivered services, or are given to your customers as part of consulting and services engagements.
- The location of all open source code repositories used in development, with strict rules about what code with which licenses can be combined (or not).

## What you then need to put in place

- Uniform cross-organizational rules and policies about the use of open source, with the ability to audit adherence.
- Tools to determine code provenance: from which original bodies of open source code did your current codebase derive?
- Balanced policies to weigh the business and legal benefits and risks in using open source code.

## What you then need to put in place

- Education for all employees and contractors, with special sections appropriate for users, contributors, developers, and distributors of open source code.
- Clear processes defining when decisions about open source can be made locally and when they must be made centrally, with paths for escalating decisions going up both the executive and legal chains.
- An aggressive policy for contributing to the various open source communities from which you benefit in your company or organization.

## The IBM experience

- Ten+ years contributing to and leading hundreds of open source projects in efforts such as Linux, Eclipse, and Apache.
- An internal governance process embodied within the Open Source Steering Committee (OSSC), with the set of rules now in their third generation in the last decade.
- The OSSC reviews all IBM external activities involving Open Source including
  - Starting a new OSS community/project
  - Contributing to an existing OSS community
  - Using OSS in IBM products or services
  - Distributing reference implementations or OSS modifications
  - Redistributing (OEM or Resell) vendor products containing OSS

## Use of open source has grown

- We have seen proposals to the OSSC grow steadily.
- The proposals fall into 3 categories
  - Already evaluated and approved for use
  - Meets well-defined criteria and a centralized committee can handle
  - Complex or original scenarios that are best decided by top of the business
- The governance process continues to evolve
  - Scalability: handle increase in the number proposals
  - Delegation: allow business units to drive majority of decisions
  - Economy: don't spend money on people and resources to answer questions to which you already know the answers.

## Some lessons learned

- We were worried about code quality but we shouldn't have been.
- We gained a better understanding of the open source domain
  - Copyright and patent complexities
  - License terms and conditions
  - Usual lack of warranty
- We learned to balanced open and proprietary.

## Some lessons learned

- We gained a better understanding of the value of open source
  - How to leverage it in what we do
  - How and where to contribute
  - How to work well in open source communities
- We learned to manage the risks.
- We learned it is important to have clear business and strategic reasons for using open source

## Final thoughts

- Develop your open source policy collaboratively among your business, technical, and legal experts, don't dictate it.
- Education is key for employee and contractor compliance.
- Establish clear policy for what employees can and cannot do with open source in their spare time.
- Consider using code pedigree and scanning services from companies such as Black Duck, OpenLogic, and Palamida.
- Know where handling open source needs to be the same as closed source, and where it needs to be different.
- Plan to iterate on and refine your policy yearly for the first few years.