Sep 21, 2017

I3PM GA

Speaker: Philippe Therias

Sample Free & Open Source Software ("FOSS") company management processes

PHI IP AVOCATS

FOSS : a def nition for our purposes

- Software easily (no technical hurdle) downloadable from the internet

- In human-readable (« source ») form

- No money involved

In software world, copyright reigns... yet copying is the norm !

- FOSS is pervasive and growing in commercial and home-grown software (« eating the software world »)

- many authors / contributors / communities around the globe on the internet
- 2011 Gartner finding that more than 50% of surveyed IT organizations use FOSS (from 10% in 2006)
- 2016 Gartner predicts by 2018 70% of new apps will run on FOSS databases
- « Gartner asserts that open source components are present in more than 95% of a business' applications and over 30% of most code bases »
- 2016 Northbridge/Back Duck findings :
  - less than 3% of surveyed companies do not use FOSS
  - the foundation for nearly all applications (80-90% of code), operating systems, cloud computing, databases, and big data

- Generally accepted principle that software (including FOSS) is protected by copyright

Reminder of prerogatives of FOSS owners

- Unless exception FOSS continues to have a copyright owner : author or assignee has not surrendered its rights

- Prerogatives of FOSS owner in most countries:

  - by law : prevent others from using, copying, modifying, distributing

  - by contract (license) :

    - permit part or all of using, copying, modifying, distributing

    - on additional conditions as the case may be

Encountered FOSS situations

Any of :

- clear public domain declaration by true owner
- one of the (currently 83) Open Source Initiative « standard » licenses* : all very permissive (to use, copy, modify, distribute), but with or w/o cumbersome additional conditions / obligations

*https://opensource.org/licenses/alphabetical

- license « made up » by owner
- no license to be found
- doubts about the true owner
- embedded software and dependencies

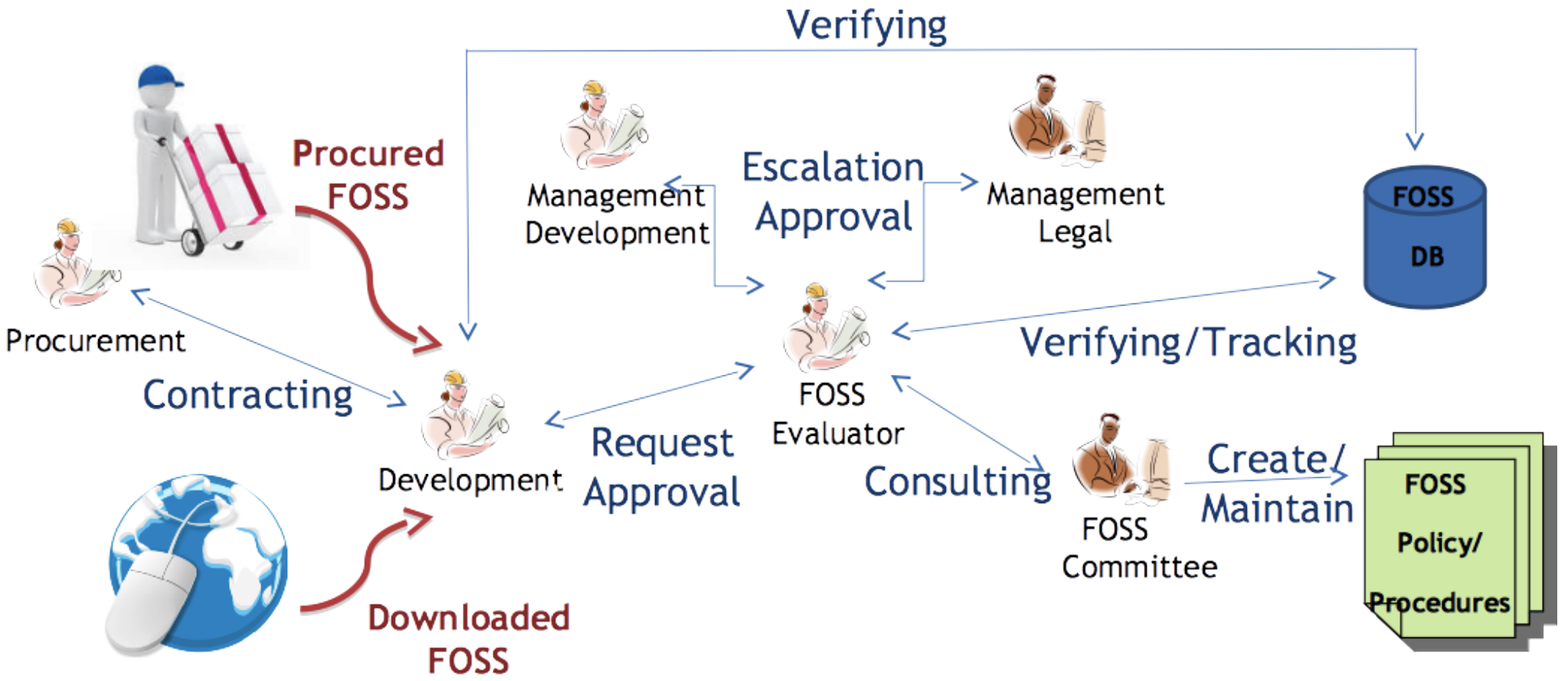
Possible risks tackled by a FOSS company management process

- Using FOSS without license, or with license but not meeting all additional obligations, exposes to copyright infringement
  - Theoretical risk: statutory/actual damages, injunction, reputation
  - FOSS is litigated by big players (ex : Free Software Foundation and Linux), only ?

- Other possible risks :
  - Infringement of patents (using, distributing)
  - Surrendering own IP rights unwillingly (distributing)
  - Technical security and vulnerability (using, distributing)
    - what if vulnerability compromises personal data ?
      https://www.theregister.co.uk/2017/09/20/equifax_vulnerability_could_be_widespread/

- With never any warranty or indemnification !
  - all liability is entirely with the user/distributor

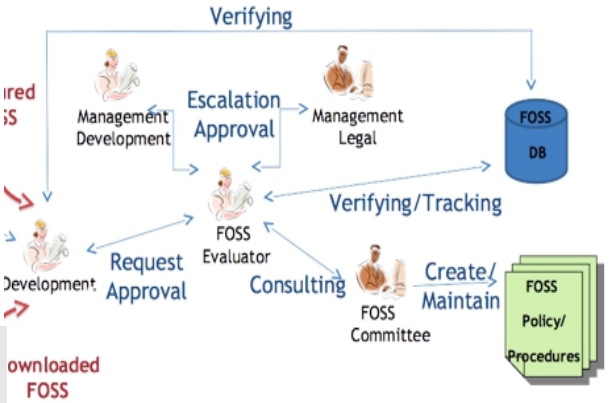
Commonalities between sample FOSS management process f bws



Certain differences

	BigCo	MidCo	SmallCo
Developers can download from a in-house repository of “known” FOSS	Yes	No	No
FOSS downloaded from internet is code scanned; “Unknown” FOSS undergoes a pedigree review	Yes	No	No
Product development process includes FOSS-related steps verified by Attorney	Yes	No	No
Procured software is code scanned (except Linux etc.)	Yes	No	No
Supplier’s list of FOSS is reviewed	Yes	Yes	No

Certain differences (2)



	BigCo	MidCo	SmallCo
Certain “unknown” FOSS undergo verification that no applicable own patent	Yes	Yes	No
FOSS approval is for specific product and specific usage	Yes	No	No
Tracking tool allows to know all products in which FOSS is included	Yes	Yes / No	No
Product is code scanned before public release	Yes	Yes / No	No
Product packaging is checked for compliance with FOSS licenses by Attorney	Yes	No	No
Vulnerability in FOSS is constantly monitored and FOSS remediated in products	Yes	Yes / No	No

What is the right FOSS management process for your company ?

- 2014 Gartner Survey Analysis: Open-Source Software Adoption and Governance : « only one-third of respondents have a corporate policy to **govern** use and purchase of FOSS in the enterprise »
- 2016 Northbridge/Back Duck findings :
    - 50% of companies surveyed have no formal policy for **choosing** open source code
    - 47 percent have no formal process in place to **track** open source code
    - nearly one-third of companies have no process for **identifying**, **tracking** or **remediating** known open source vulnerabilities
- 2017 BlackDuck Survey Analysis : Open Source Security and Risk Analysis: 96% of the analyzed commercial applications contained open source code, and more than 60 percent contained open source security vulnerabilities