Implementation of a FOSS License Compliance Program

Coscup/GNOME Asia 2010

Soeren Rabenstein (石書任)
ASUSTeK Computer Inc.
Legal Compliance Department

August 14, 2010

Syllabus

- ◆ Top 6 Misjudgements
- ◆ Compliance Program
- ◆ Tools
- ◆ Mistakes to Avoid

Top 6 Misjudgments

1. “We don’t use FOSS”

   In fact, most products involve FOSS, e.g.

   – Linux used in the majority of embedded devices

   – ~ 70 % of the Internet runs on FOSS

   – Mobile platforms: Symbian, Android, WebOS, MeeGo

   – MacOSX/NEXTSTEP based on BSD

   – even Windows 7 contains FOSS

Top 6 Misjudgments (Cont.)

2. “Open source licenses are not enforceable or at least not enforced, so we don’t need to worry about license compliance”

Many court decisions, e.g.

- Welte./. Skype (Munich)
- Jacobsen ./. Katzer (Northern California)
- SFC ./. Samsung, WD, Best Buy, JVC, Bosch, Zyxel, Westinghouse, Phoebe, and others (last December, New York)

Top 6 Misjudgments (Cont.)

3. “Customers don’t care about our use of open source”
   - The copyright holders are amongst the consumers
   - Organizations like gpl-violations.org act based on specific complaints… there are many
   - Products are exposed to the market, you cannot hide
   - End-user-brand companies face big risks, will push it up the supply chain

Top 6 Misjudgments (Cont.)

4. Somebody else takes care of it
   - “The legal department will take care of it”
   - “The engineering department will take care of it”
   - “The supplier will take care of it”

Top 6 Misjudgments (Cont.)

5. “We use so little open source software that we can handle it informally”
   - If you do not manage it, you cannot know how big or little it is
6. “We are using FOSS for ‘Software as a Service’ (SaaS) applications only, so open source licenses obligations won’t apply”

   Not true for:
   - AGPL
   - M&A

Compliance Program

Open Source is ubiquitous

1. Needs to be managed
2. Process implementation is critical

Compliance Program (Cont.)

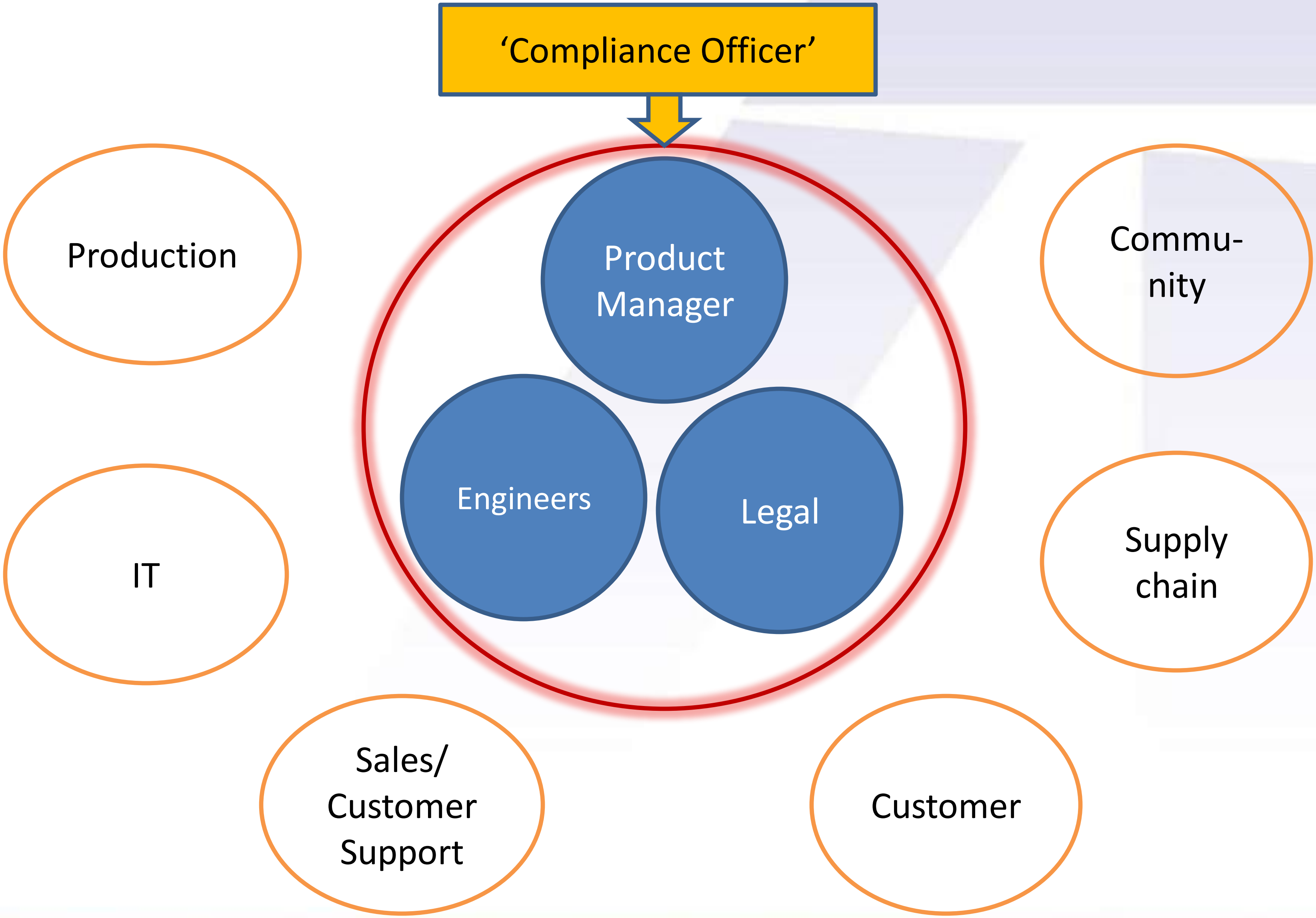
- Appoint central person for overall compliance
- Get managements support
- Analyze current FOSS use
- Review licenses
- Define approved uses
- Delegate tasks/responsibilities
- Set-up SOPs that integrate with the existing workflows (verify, get feedback and revise)
- Publish policies/SOPs
- Educate employees
- Improve and control

Compliance Program (Cont.)

Required Processes

- Code management
- License management
- Inbound compliance
- Release management
- Outbound compliance
- Violations

Compliance Program (Cont.)



'Compliance Officer'

Product Manager

Engineers

Legal

Production

IT

Sales/ Customer Support

Customer

Commu- nity

Supply chain

Compliance Program (Cont.)

Avoid external miscommunication

- Publish a dedicated contact window
- Enlist your compliance program with the Linux Foundation’s Compliance Directory

http://www.linuxfoundation.org/services/compliance/directory.

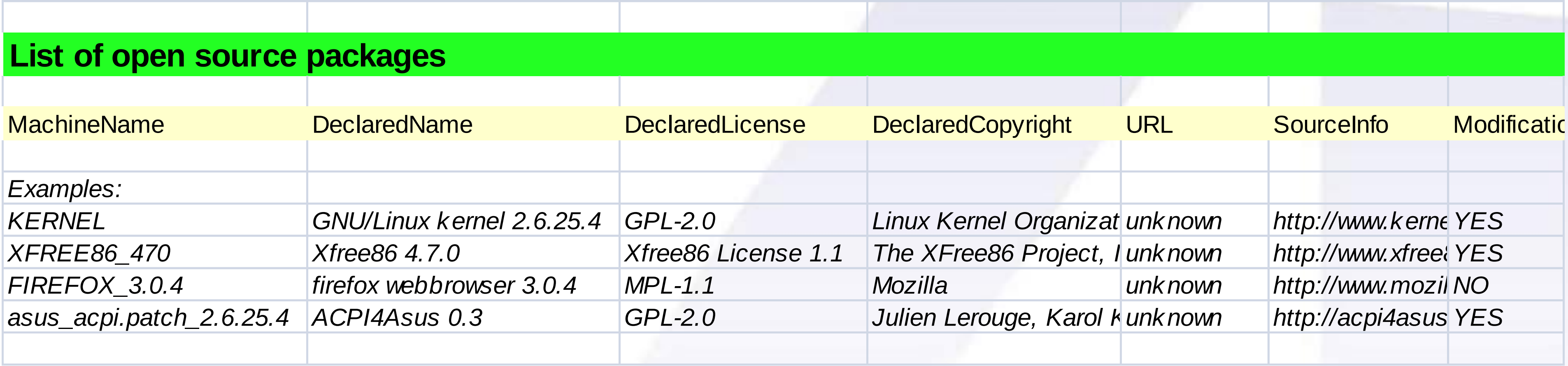
Tools (cont.)

“Software BOM” or “Bill of Code”

- ‘List of ingredients’
- … and their respective licenses
- Code management essential
- Control document for compliance
  - Checklist for inbound compliance
  - Checklist for source code release
  - Checklist for license texts
- Product documentation for B2B customer

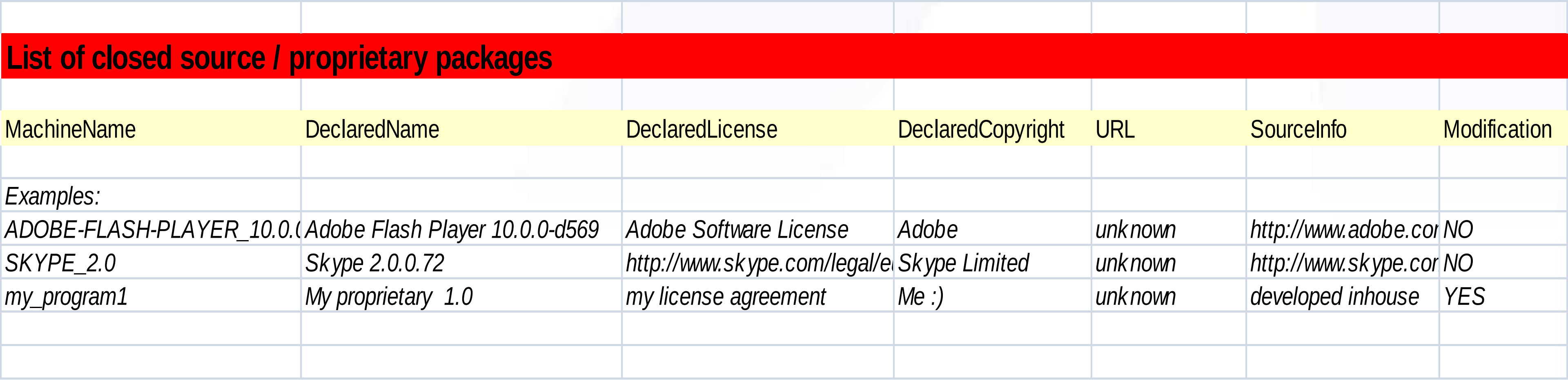
Tools

“Software BOM” or “Bill of Code”



List of open source packages

MachineName	DeclaredName	DeclaredLicense	DeclaredCopyright	URL	SourceInfo	Modificatic
Examples:						
KERNEL	*GNU/Linux kernel 2.6.25.4*	*GPL-2.0*	*Linux Kernel Organizat*	*unknown*	*http://www.kerne*	*YES*
XFREE86_470	*Xfree86 4.7.0*	*Xfree86 License 1.1*	*The XFree86 Project, I*	*unknown*	*http://www.xfree8*	*YES*
FIREFOX_3.0.4	*firefox webbrowser 3.0.4*	*MPL-1.1*	*Mozilla*	*unknown*	*http://www.mozil*	*NO*
asus_acpi.patch_2.6.25.4	*ACPI4Asus 0.3*	*GPL-2.0*	*Julien Lerouge, Karol K*	*unknown*	*http://acpi4asus*	*YES*



List of closed source / proprietary packages

MachineName	DeclaredName	DeclaredLicense	DeclaredCopyright	URL	SourceInfo	Modification
Examples:						
ADOBE-FLASH-PLAYER_10.0.(	*Adobe Flash Player 10.0.0-d569*	*Adobe Software License*	*Adobe*	*unknown*	*http://www.adobe.cor*	*NO*
SKYPE_2.0	*Skype 2.0.0.72*	*http://www.skype.com/legal/e*	*Skype Limited*	*unknown*	*http://www.skype.cor*	*NO*
my_program1	*My proprietary 1.0*	*my license agreement*	*Me :)*	*unknown*	*developed inhouse*	*YES*

Tools (cont.)

Software Package Data Exchange™ (SPDX™) SPDX

- standard for communicating the components, licenses and copyrights associated with a software package
- Use in documents like SW-BOM/BOC
- SPDX™ to become industry standard
  - ➔Target Q4/2010
  - ➔ monitor www.spdx.org

QUALCOMM
hp
redhat
CANONICAL
Texas Instruments
freescale semiconductor
blackduck
nexB
WIND RIVER
PALAMIDA Application Security for Open Source Software
OpenLogic
APACHE
BT
SOURCE Auditor "Keeping Your Source Code Yours"
coverity
Software Freedom Law Center
mozilla FOUNDATION
eclipse
MICRO FOCUS
Alcatel·Lucent
...and others

Tools (cont.)

Source Code Scanning

Tools and Services

- Fossology
- Blackduck™ Protex
- nexB™ Software Audit
- OpenLogic™
- Palamida™
- Source Auditor™

Tools (cont.)

Further analysis tools

- Binary Analysis Tool
- Dependency Checker Tool
- Bill of Material Difference Tool
- …

First port of call:

➔ fossbazaar.org

Mistakes to avoid

- Policy/SOP need to suit workflows
- Policy/SOP must not be
  - too strict
  - too technical
  - too legal
  - unrealistic
- Ensure compliance till EOL+3years (Avoid the ‘Build Guru’)
- Be flexible, don’t just add another bureaucracy layer

Question and Answer

Thank You!