Overview of Open Source software license compliance approaches and certificates

OSADL Policy Template, OSADL Supplier/License Compliance Audit (S/LCA), OpenChain (ISO 5230)

Caren Kresse
Open Source Automation Development Lab (OSADL) eG

The OSADL Open Source Policy Template

The basis for license compliance

A FOSS policy is needed ...

... to avoid copyright infringements,

... to create and maintain **processes** within a company,

... to establish sustainable **understanding** of concepts,

... to provide **control** over licensing of a company's **own IP**,

... to meet **customer requirements**.

Open Source Policy Template

- Different companies take different approaches to license compliance, a company's FOSS policy must reflect these.
- Creating a policy requires **understanding and expertise**.
- Using a policy requires it to be **brief and specific**.

→ The **OSADL Open Source Policy Template** is structured to take these requirements into account.

Structure of the Open Source Policy Template

- Various chapters with template texts as basis for an individual policy
- Motivations and explanations for the creator of the company policy

☑ *Options to choose from where there are alternative possibilities of interpreting or handling a situation*

- text blocks to modify contracts and other documents
- *Placeholders to be filled out individually*

→ Annexes providing processes and forms for legal information

→ Supplements providing technical, legal and practical background on copyright law and license compliance.

Software flow: Input/output gateways

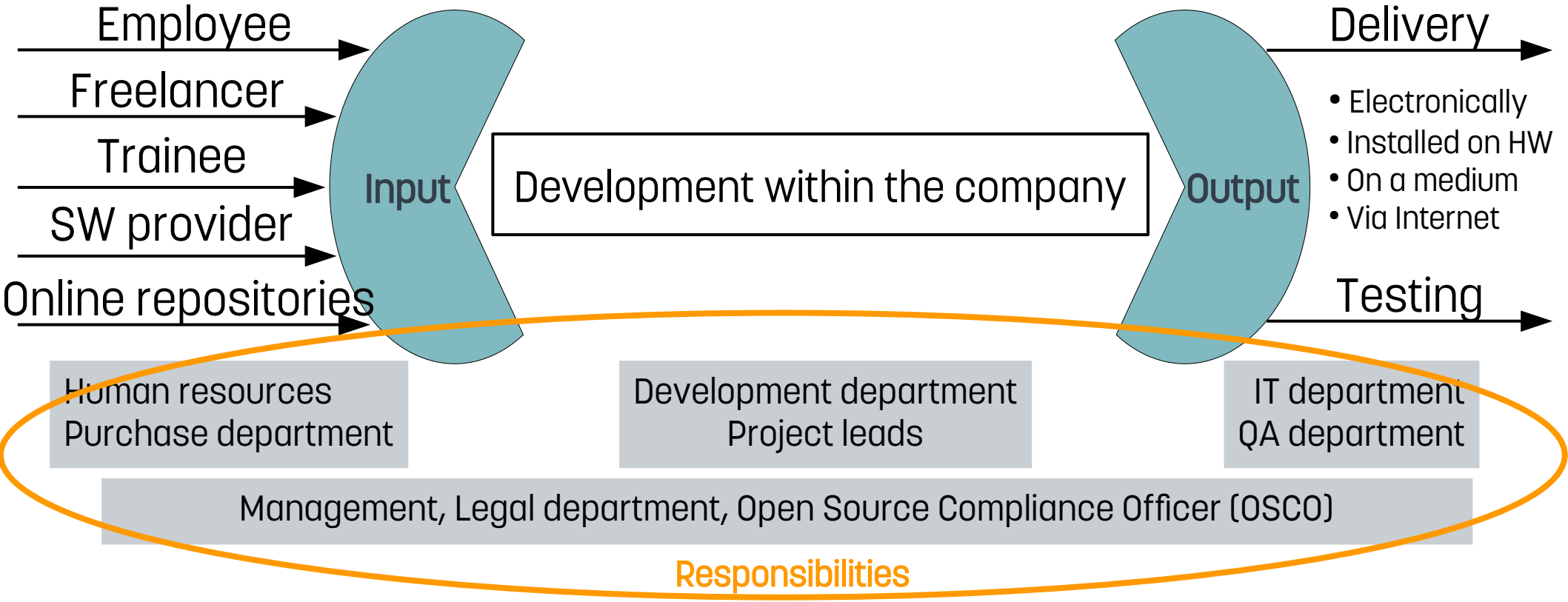
Human resources
Purchase department

Development department
Project leads

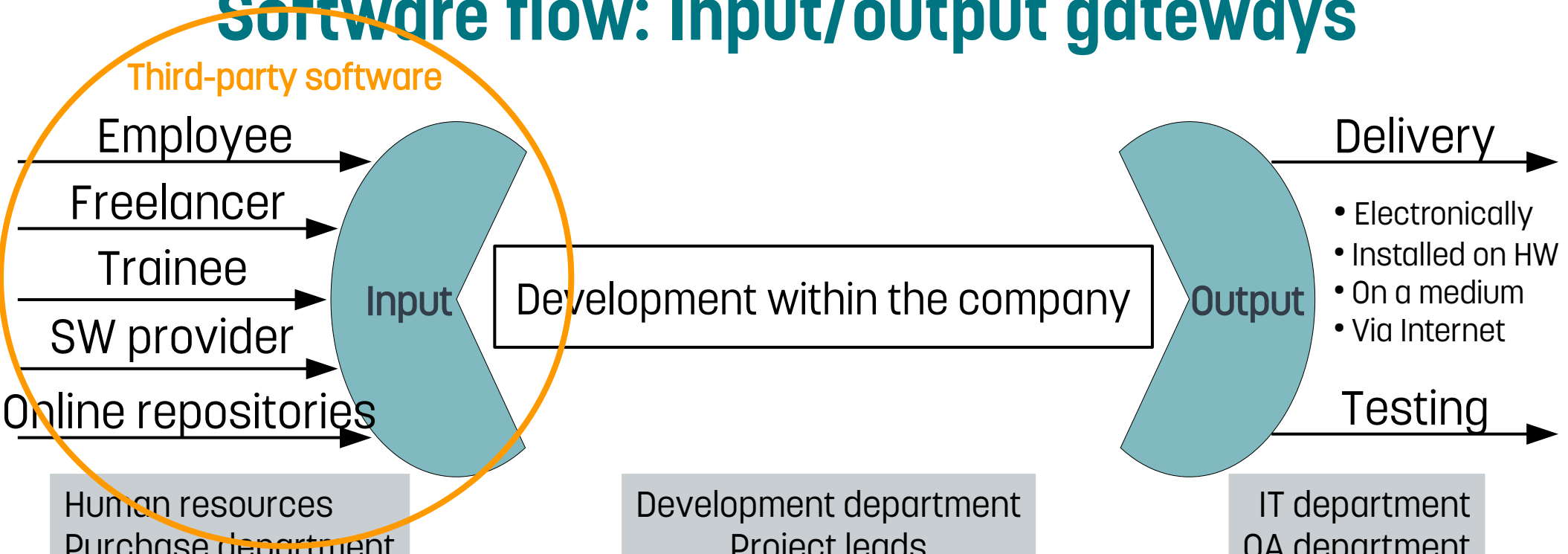
IT department
QA department

Management, Legal department, Open Source Compliance Officer (OSCO)

Software flow: Input/output gateways

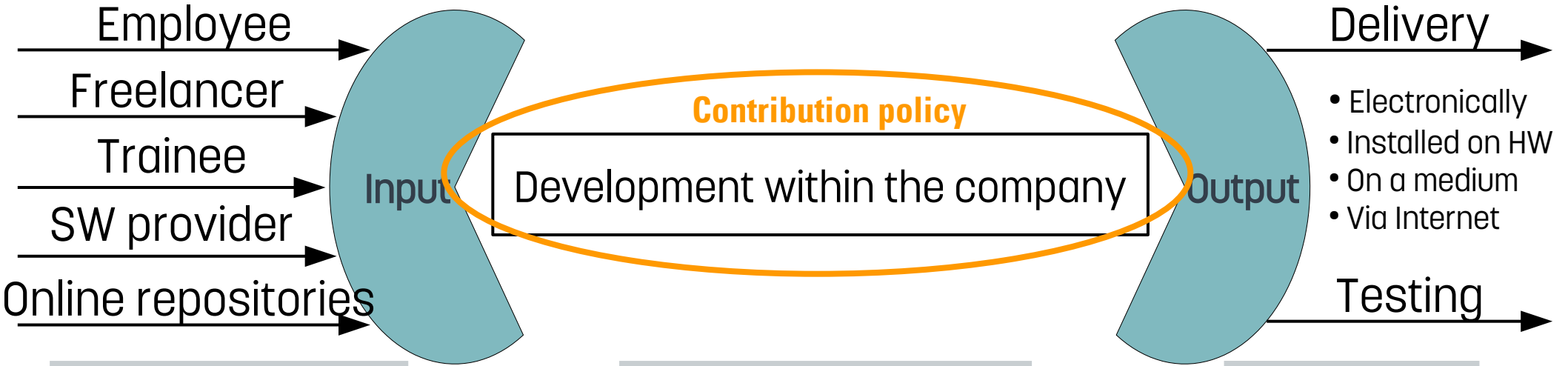


Software flow: Input/output gateways



Software flow: Input/output gateways

Software flow: Input/output gateways



Human resources
Purchase department

Development department
Project leads

IT department
QA department

Management, Legal department, Open Source Compliance Officer (OSCO)

Additional topics

- **Communication** of the FOSS Policy within the company and in employment contracts
- Selecting a suitable **license for own FOSS projects**
- **Audits and certification** (*e.g.* OpenChain, OSADL S/LCA)
- **Patent** considerations

Supplements: Background information

- Comprehensive discussion and explanation of legal, technical and practical aspects.
- As separate documents
- Among others, on:
  - **Derivative work** and **Copyleft**
  - **License compatibility**
  - **Software scanning**
  - **Rebuild** and verification of the complete corresponding source code

Build your own FOSS policy

The OSADL Open Source Policy Template is available as:

- **PDF** files on request at *info@osadl.org:*
  - A master document for the actual policy
  - Annexes and Supplements as separate files linked from the master document
  - (limitedly) editable versions without explanation boxes
- As **plain text** files on GitHub:

  github.com/osadl/foss-policy-template

I Audits and certification

To verify our compliance with FOSS license obligations and thereby evaluate our established processes, we make use of various control mechanisms. The decision on when and how often each of the following procedures is carried out depends on the content and on who can perform it.

- Review of this FOSS policy (yearly, role: OSCO)
- ISO 5230: OpenChain[4] conformance validation (yearly, role: OSCO)

> The OpenChain specification provides guidelines on what must be done to be able to distribute FOSS compliantly rather than giving specific instructions on processes. So far, conformance with these guidelines is assessed in self-evaluation. But in the future, there may be institutions that offer external OpenChain compliance audits.

- OSADL License Compliance Audit (LCA) (per product, role: OSCO, PL)

> The OSADL LCA aims to support companies to organize the compliant distribution of Linux-based embedded systems. It focuses on a specific product and in particular on the Linux kernel under the GNU General Public License (GPL-2.0) and the C library, usually the GNU C library under the GNU Lesser General Public License (LGPL-2.1). Based on the compliance requirements for these components, quality and efficiency of all compliance processes within the company are evaluated.

[4] https://wiki.linuxfoundation.org/_media/openchain/openchainspec-current.pdf

The OSADL License Compliance Audit (LCA)

Why an LCA?

- To support companies organizing the license compliant distribution of Linux-based embedded systems.
- To check the conformance with FOSS license obligations.
  - **GPL-2.0** for the Linux kernel and **LGPL-2.1** for the GNU C Library (glibc), as these licenses have the strictest obligations.
- To check license obligations with particular consideration of the required **company processes**.

Procedure

- The (L)GPL **license obligations** are checked:
  - Information obligations / distribution obligations
  - License obligations for modified software
  - Accompanying documents
  - Special obligations of the LGPL
  - Tivoization
- A report with the results and possible hints to causes of faults is created.

LCA report

- *License obligation*
  - Result
  - (Causes of fault)
  - (Elimination of fault)
  - (Possible improvements)
  - Conclusion
- Find an actual LCA report (anonymized) on https://www.osadl.org/Legal-Assessments (OSADL Member login required)

Certificate

- *License obligation*
  - Result
  - (Possible improvements)
  - Conclusion

Supplier License Compliance Audit (SLCA)

COOL COMPACT OSADL ONLINE LECTURES

OSADL Policy Template, OSADL Supplier/License Compliance Audit (S/LCA),
Open Chain (ISO 5230)
Compact OSADL Online Lectures, November 17, 2021

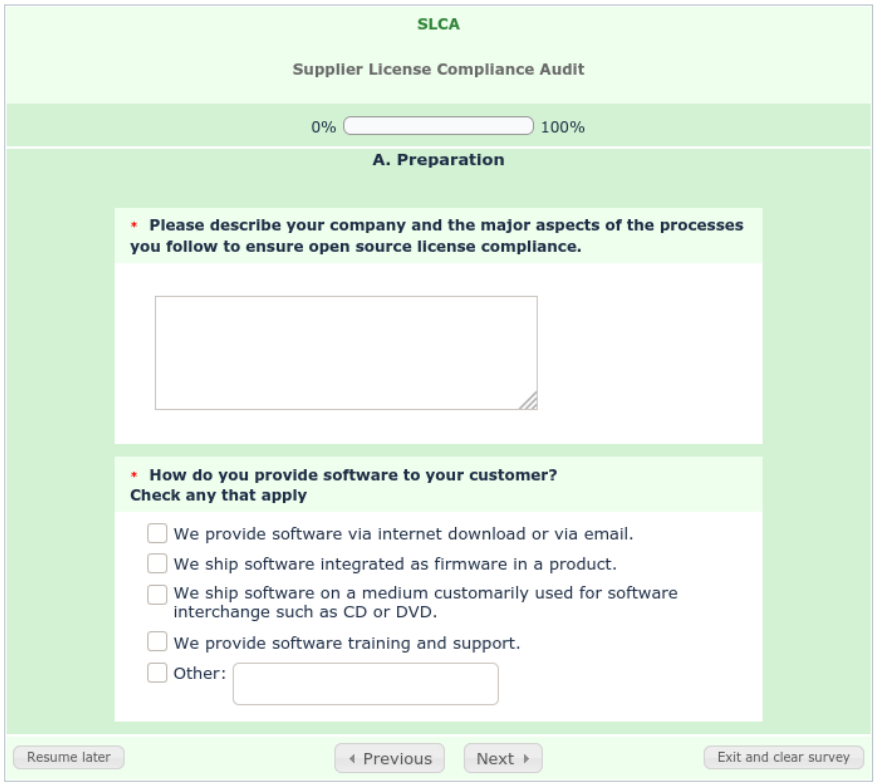
OSADL

SLCA: Online questionnaire

https://www.foss-slca.org/ (osadlmember:h3bAlp5bM)

- Questions to evaluate a company's processes that are relevant for FOSS license compliance.

SLCA: Online questionnaire (2)



SLCA: Online questionnaire (3)

A. Preparation
B. Use Case Scenario
C. Questions
   I. Organization
      1. Repository
      2. **Internal Organization/Roles/Responsibilities**
      3. Education
   II. Participation and Collaboration
      1. Participation
      2. Collaboration
      3. Exchanging Software
      4. Merger & Acquisition
   III. Incoming Code
      1. Provenance of code
         a. Downloading FOSS
         b. Incoming FOSS from other sources
      2. Form of code
      3. Inspection and Approval
      4. Licenses of incoming FOSS code

SLCA: Online questionnaire (4)

IV. License Obligations
    1. Checking for Applicable Licenses
    2. Identifying License Requirements
    3. License Texts
    4. Source Code
    5. Copyright Notices
    6. Modification Information
    7. Application Service Provider/Software as a Service

V. Handling Copyleft Licenses and License Compatibility
    1. Copyleft Licenses
    2. License Compatibility

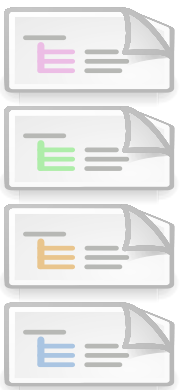
VI. Outbound Licensing and Product/ Software Solution review

VII. Maintenance Handling

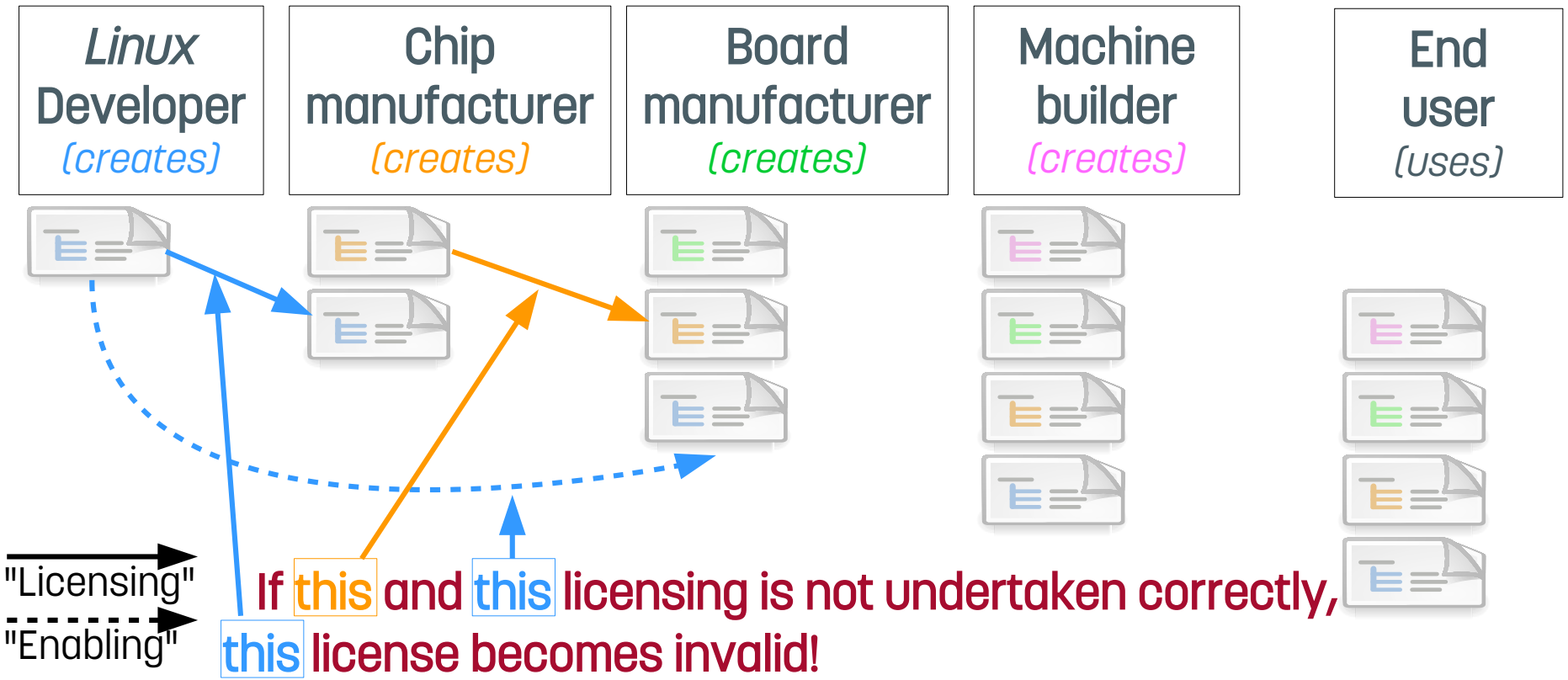
VIII. Patent Issues

OpenChain (ISO/IEC 5230)

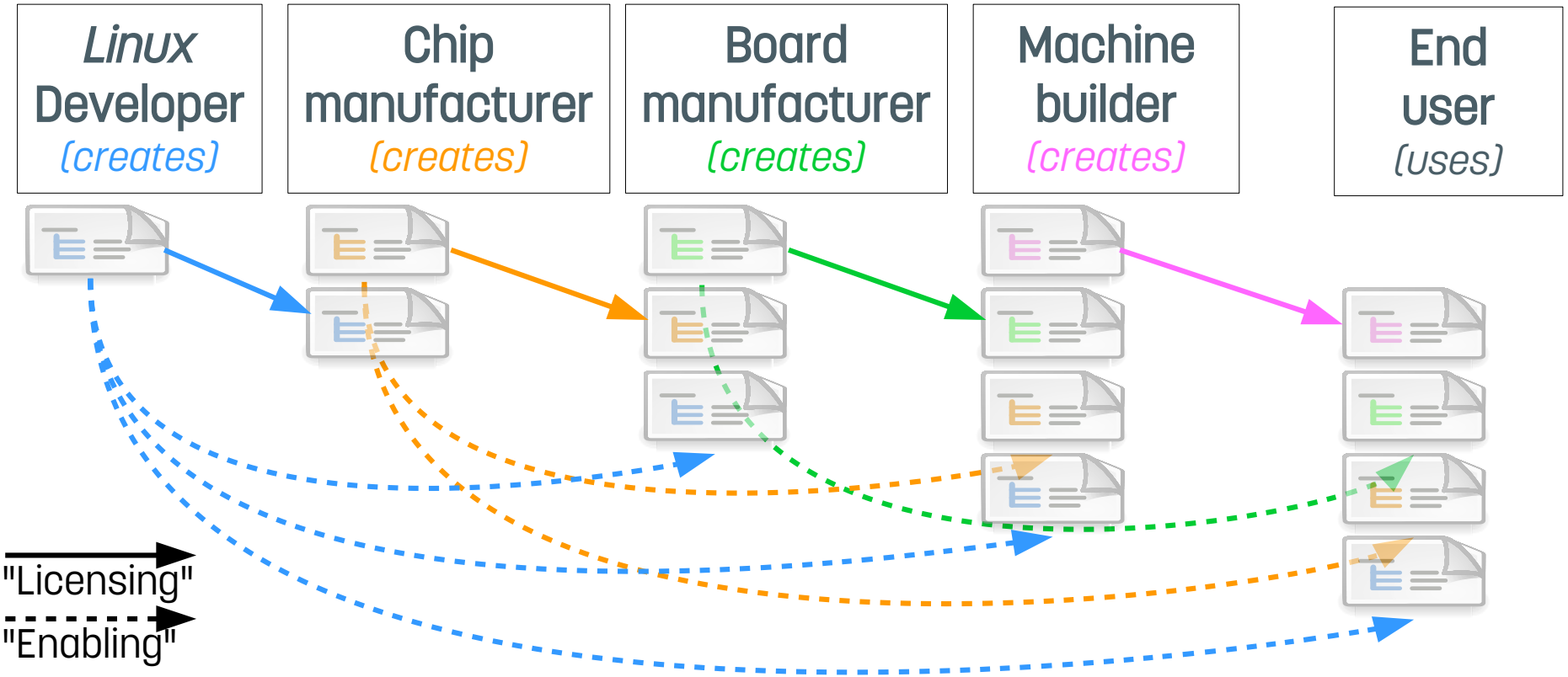
Why supplier compliance?

Linux Developer *(creates)*	Chip manufacturer *(creates)*	Board manufacturer *(creates)*	Machine builder *(creates)*	End user *(uses)*
				

Software trade chain



Software trade chain (all)



OpenChain

https://www.openchainproject.org/

- Aim: A “chain of trust” for FOSS compliance
- OpenChain provides
  - Compliance specifications
  - Training material
  - Policy template
- Self-certification or third-party certification