License Compliance Policy

Current status of the OSADL Open Source Policy Template

Caren Kresse
Open Source Automation Development Lab (OSADL) eG

Some information on today's COOL session

- Subsequent **online discussion** via video conference:
  - *osadl.org/OD-COOL (OnlineDiscussion)*
  - complete meeting URL: *https://jitsi2.osadl.org/OSADLCOOL*
- **Ask questions:**
  - *osadl.org/Questions-COOL* or *info@osadl.org*
- Please leave **feedback:**
  - *osadl.org/Feedback-COOL*

What is "Free and Open Source-Software" (FOSS)?

- Software whose **license** fulfills specific requirements is called "Free", "Open Source" or "Free and Open Source".
- Unrestricted and unconditional permission to **run, analyze and modify** the software
- **Copying and distribution** are permitted provided that **license conditions** are complied with

What is company compliance?

- Compliance with legal provisions and regulations
- Compliance with standards
- Compliance with ethical requirements

What is company compliance?

- Compliance with legal provisions and regulations
- Compliance with standards
- Compliance with ethical requirements

Copyright law

To prevent copyright infringement, protected works may only be copied and distributed when a valid license is obtained.

Who is responsible for company compliance?

The legal representative of a company...

Who is responsible for company compliance?

Not the employees.

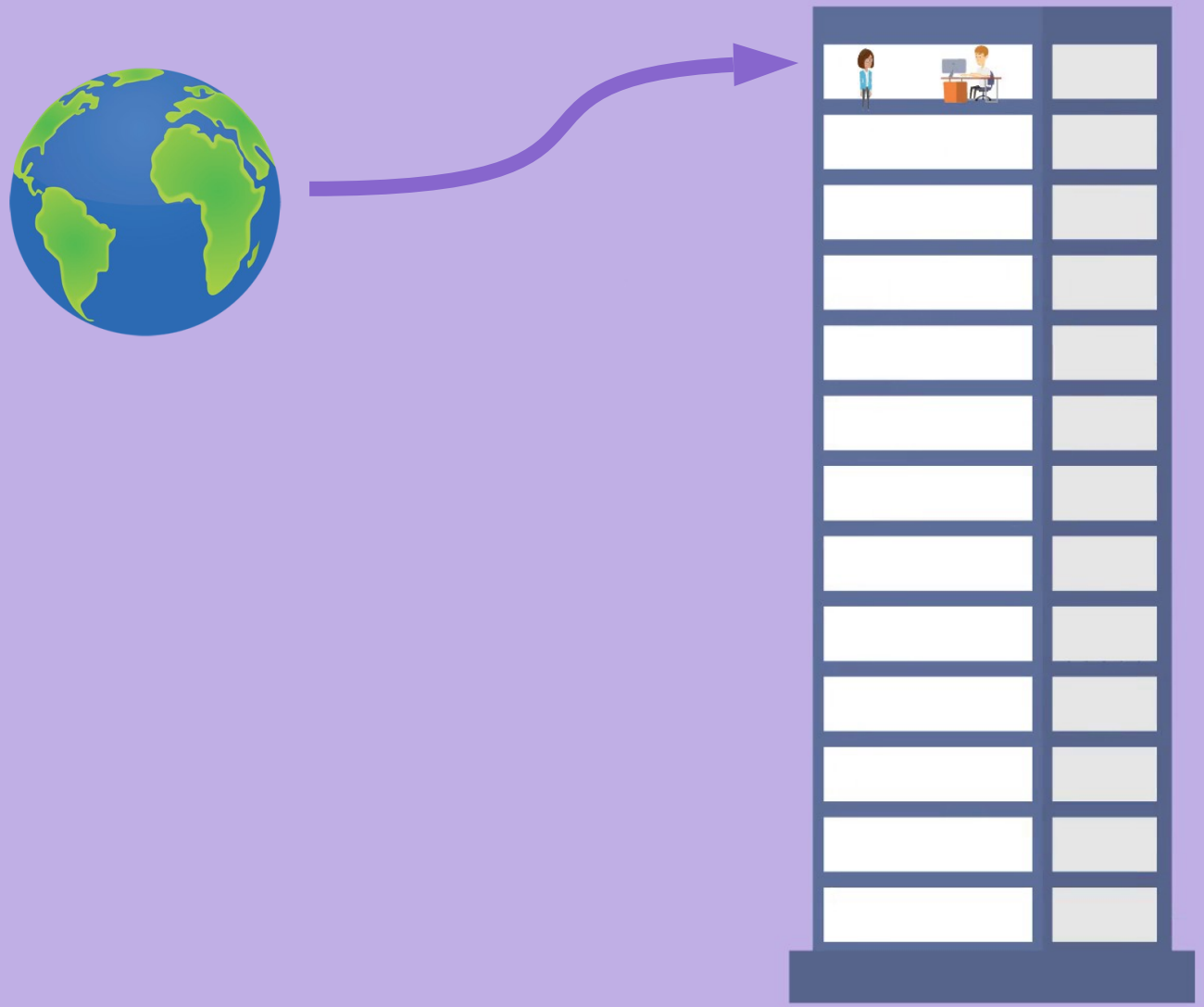
But the **management!**

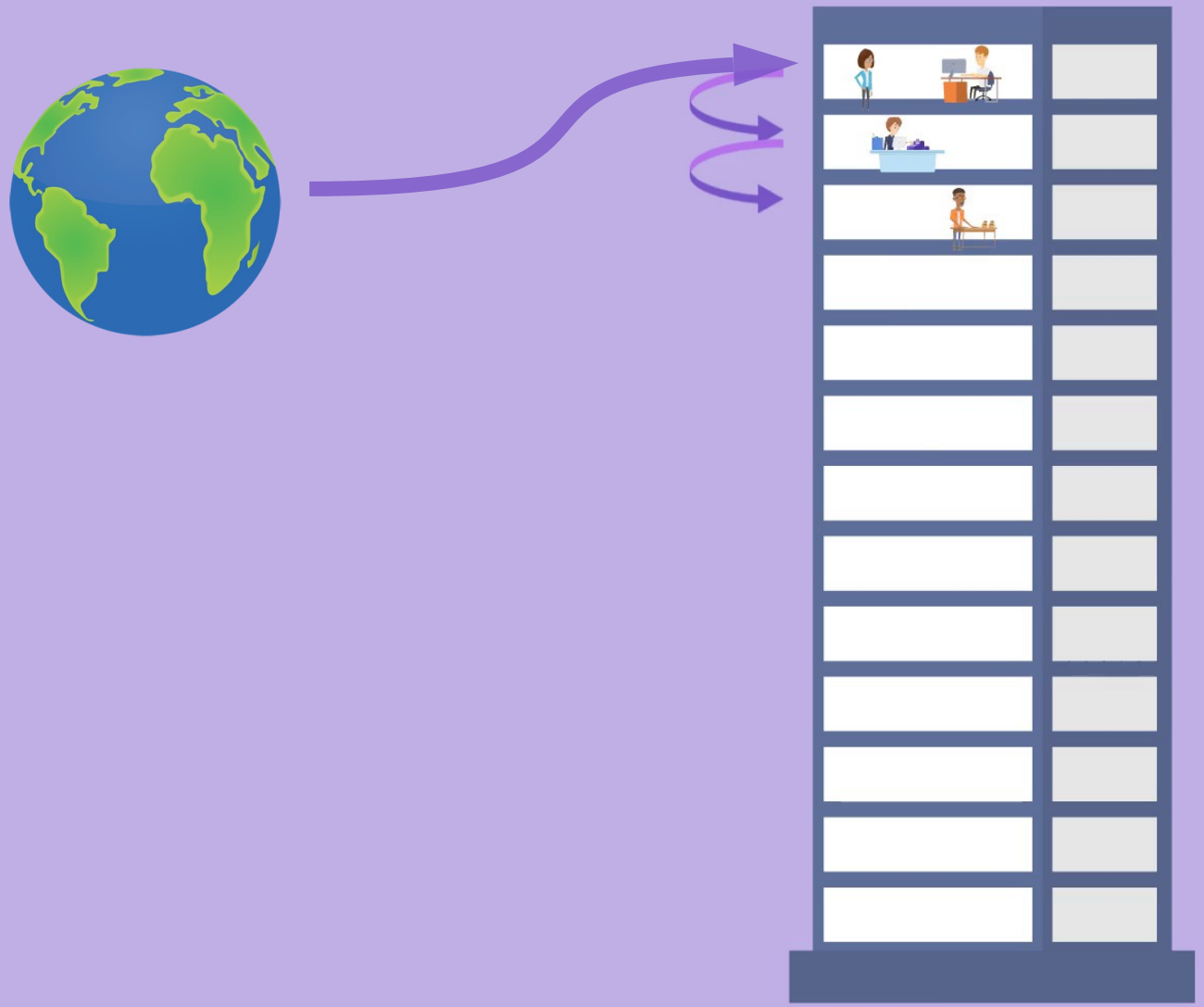
Who is responsible for company compliance?

Not the employees.

But the **management!**

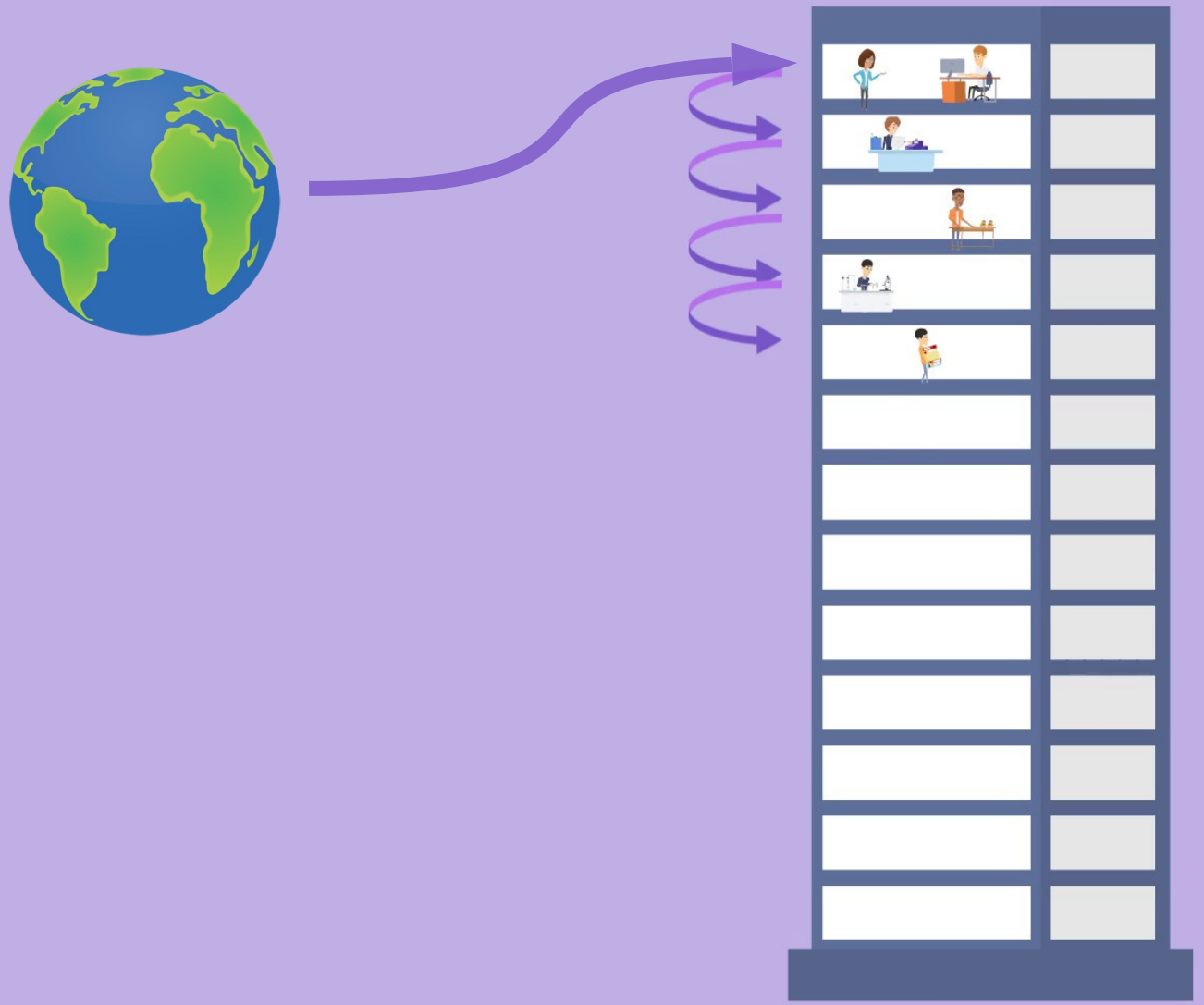
How do new strategies normally enter a company?


Management



Management

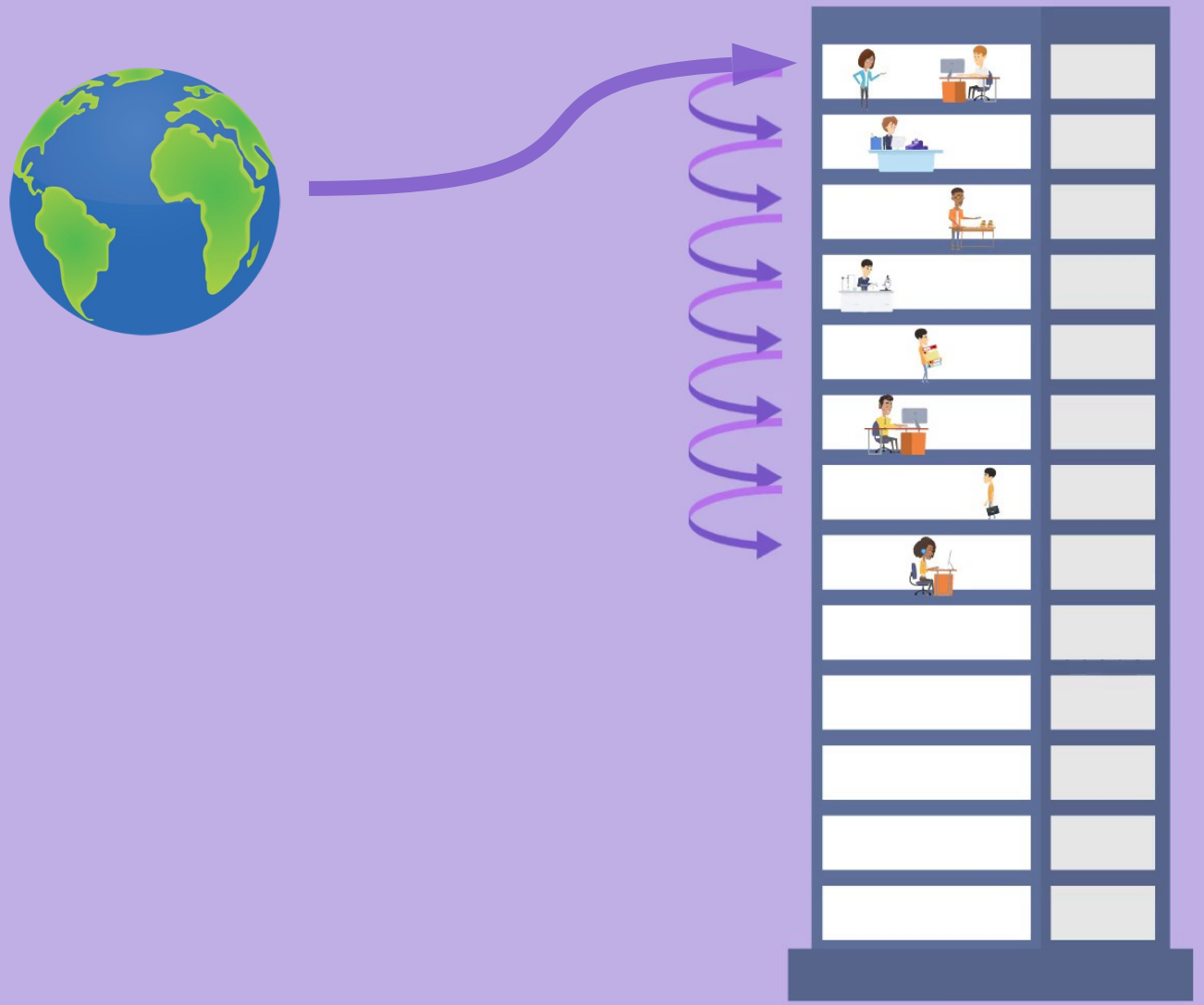
Strategic management



Management

Strategic management

Research and Development

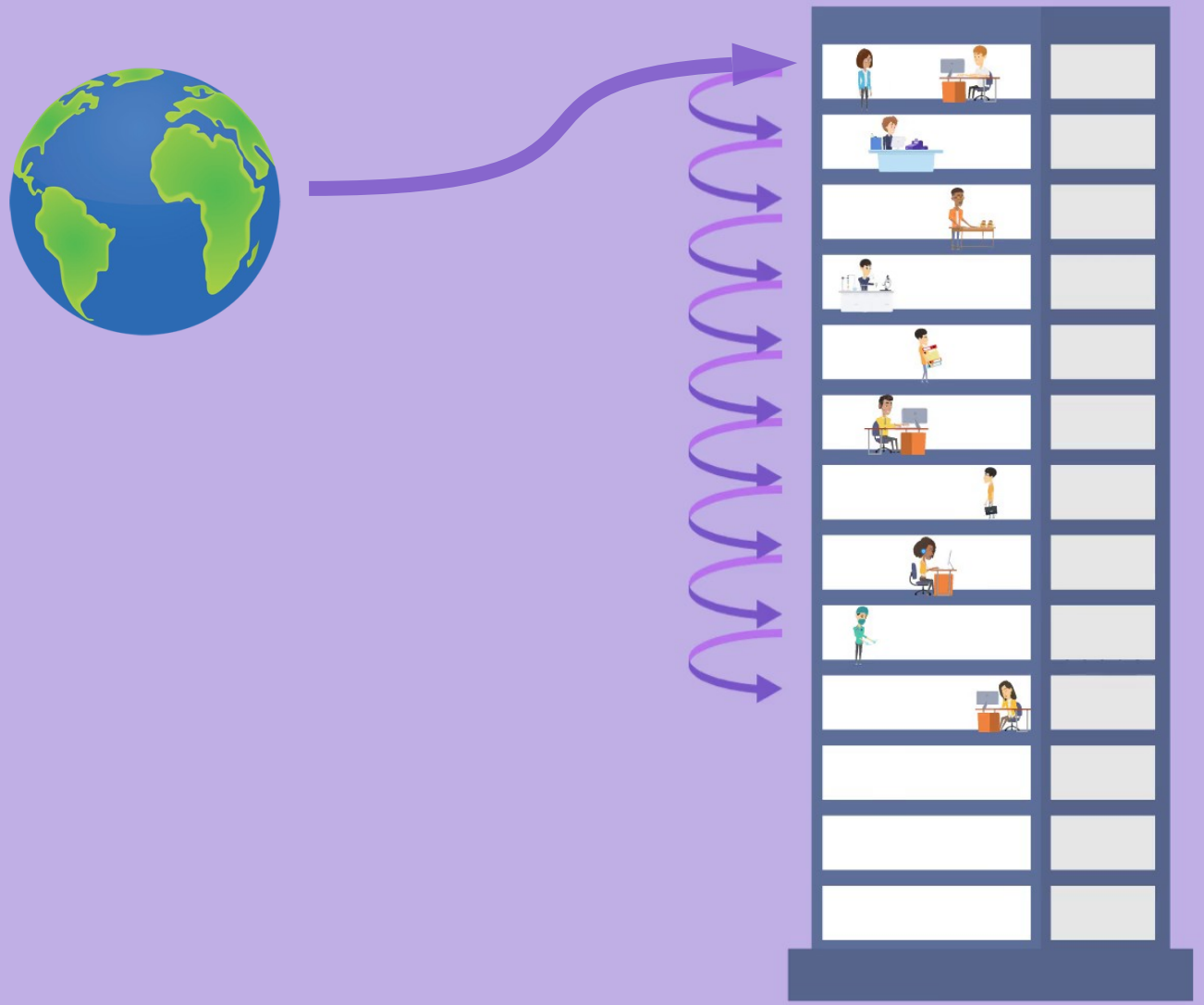


Management

Strategic management

Research and Development

Product management



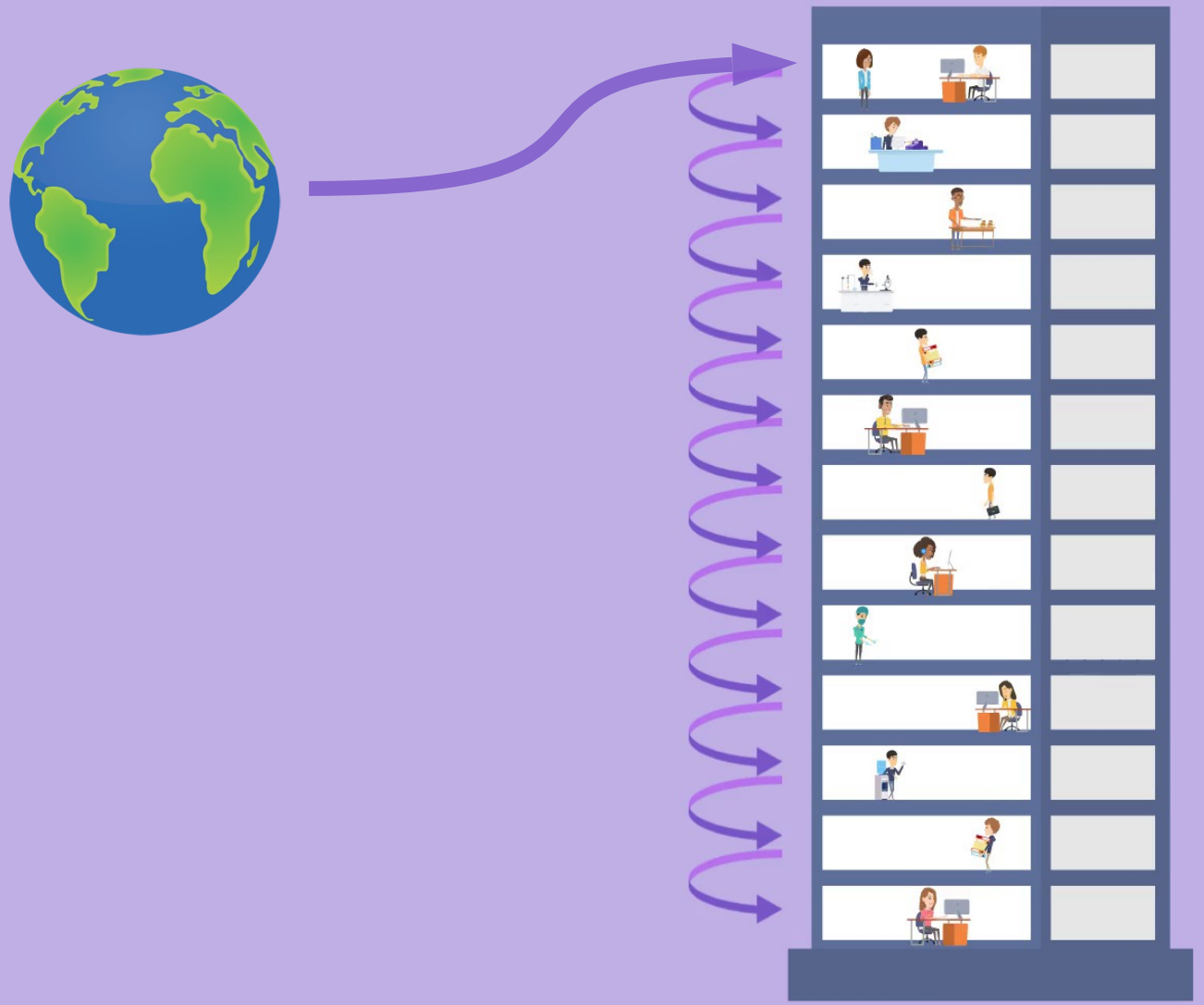
Management

Strategic management

Research and Development

Product management

QA department



Management

Strategic management

Research and Development

Product management

QA department

Software development

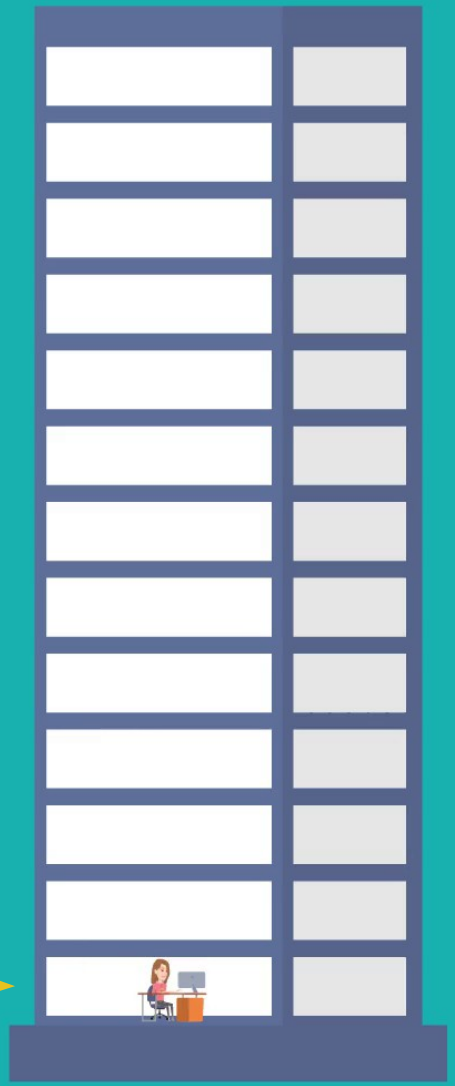
How does *Open Source* normally enter a company?

COOL COMPACT OSADL ONLINE LECTURES

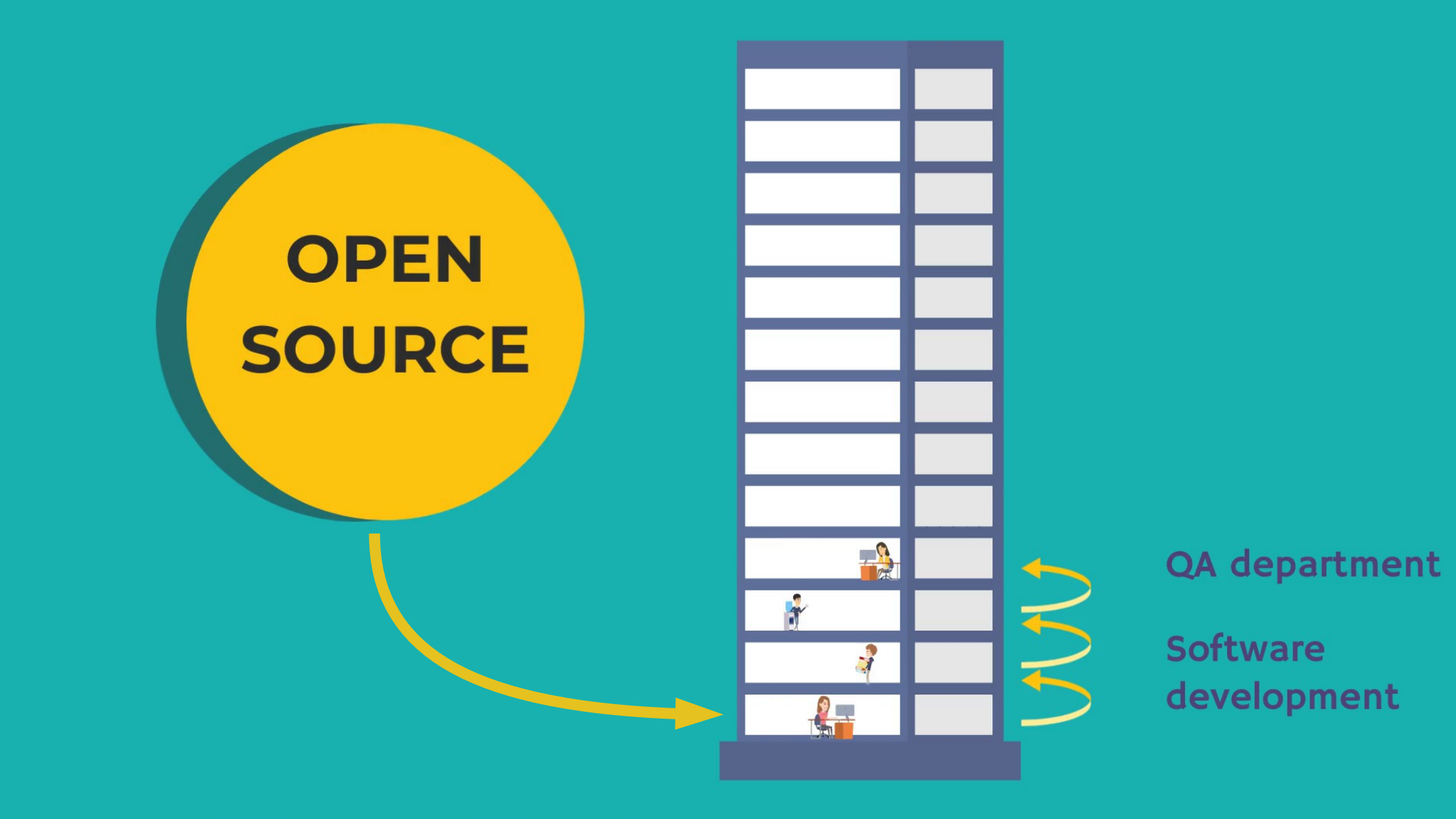
License compliance policy
Current status of the OSADL Open Source Policy Template
COOL February 24, 2021

OSADL Open Source Automation Development Lab eG

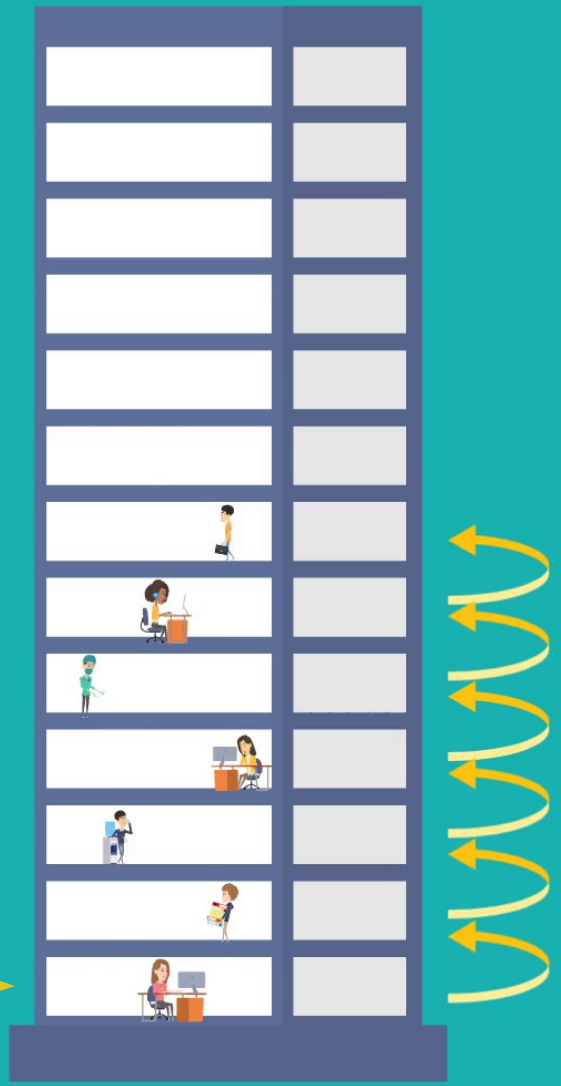
OPEN SOURCE



Software development


OPEN
SOURCE
QA department
Software
development

OPEN SOURCE

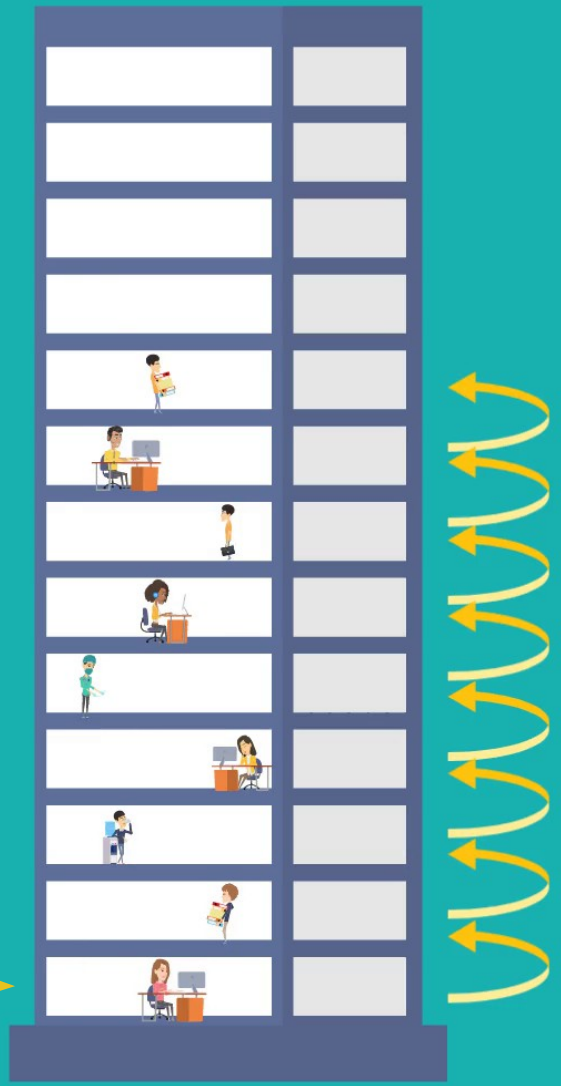


Product management

QA department

Software development

OPEN SOURCE



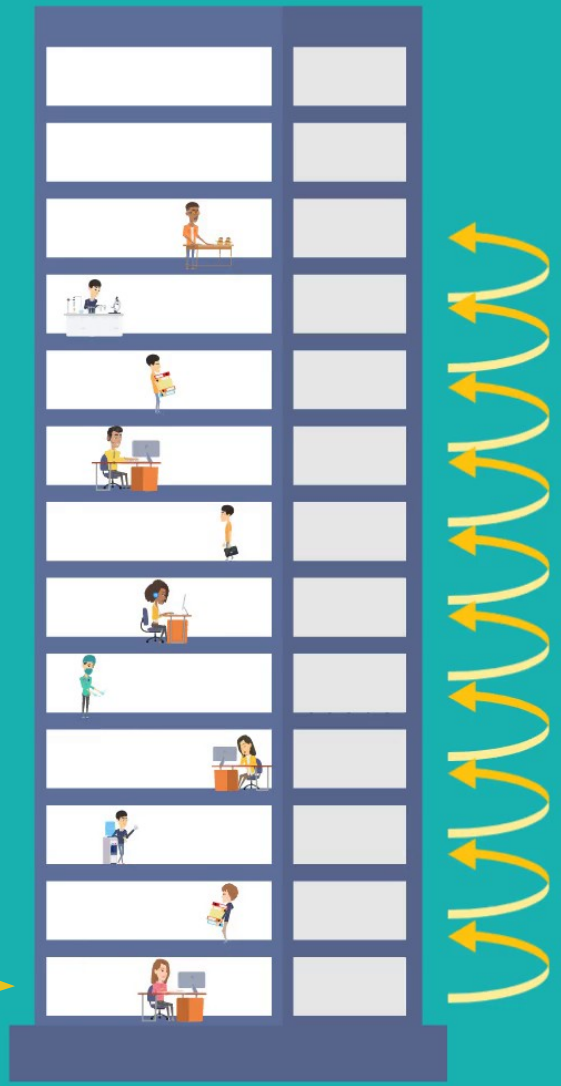
Research and Development

Product management

QA department

Software development

OPEN SOURCE



Strategic management

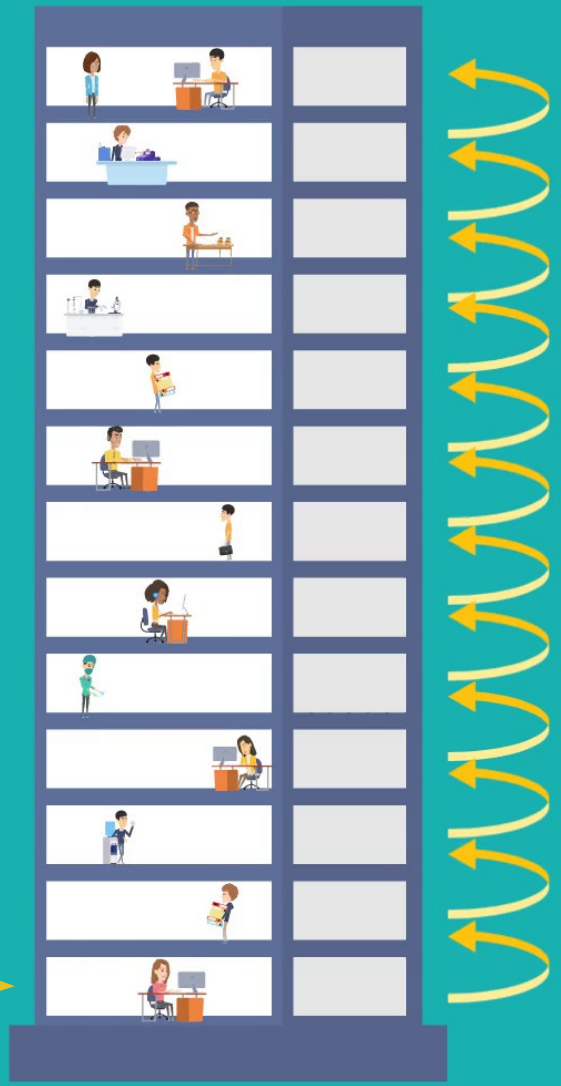
Research and Development

Product management

QA department

Software development

OPEN SOURCE



Management

Strategic management

Research and Development

Product management

QA department

Software development

OPEN SOURCE

COMPLIANCE IS A MATTER OF THE BOSS!

Management

Strategic management

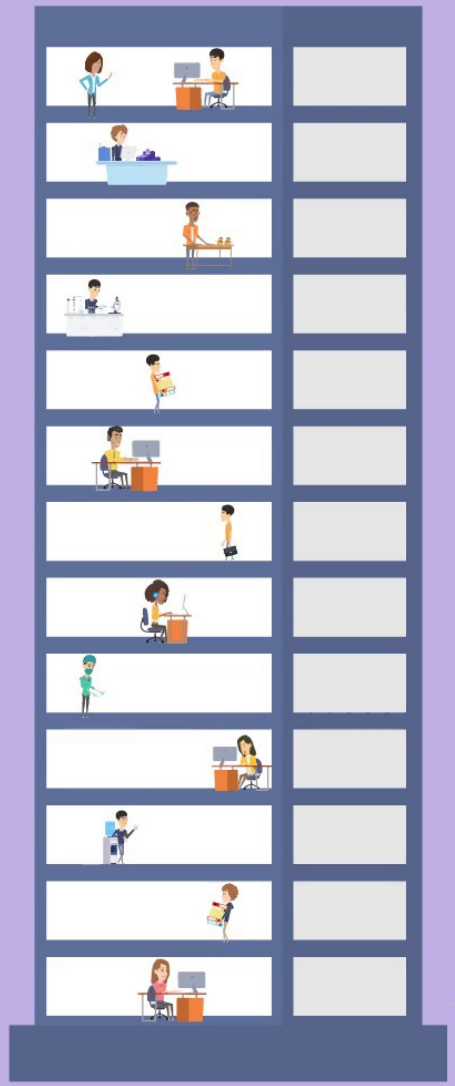
Research and Development

Product management

QA department

Software development

Open Source needs *both* ways



Management

Strategic management

Research and Development

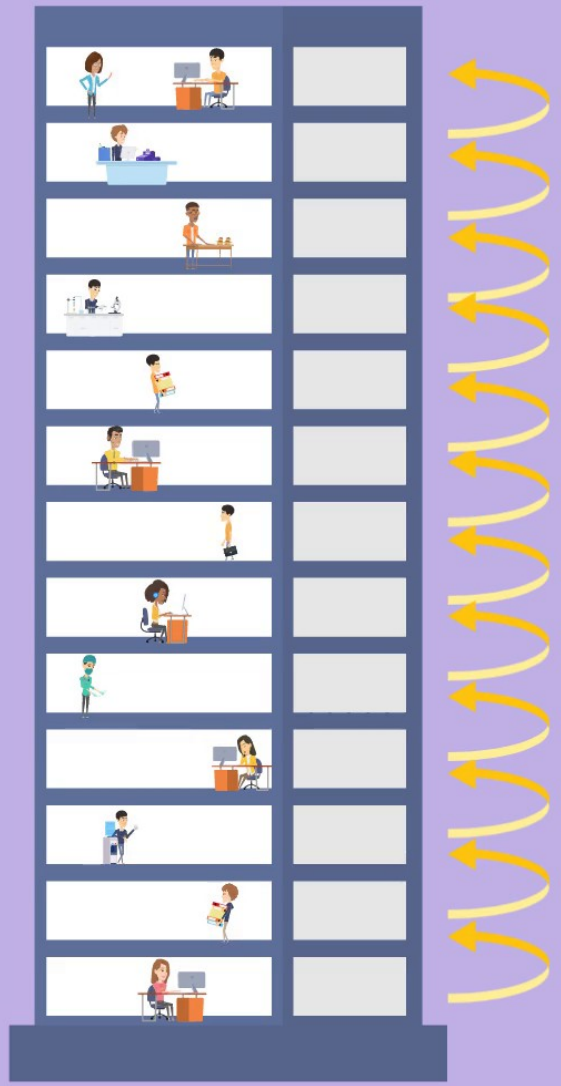
Product management

QA department

Software development

Open Source needs *both* ways

- The comany must be aware that Open Source is used.



Management

Strategic management

Research and Development

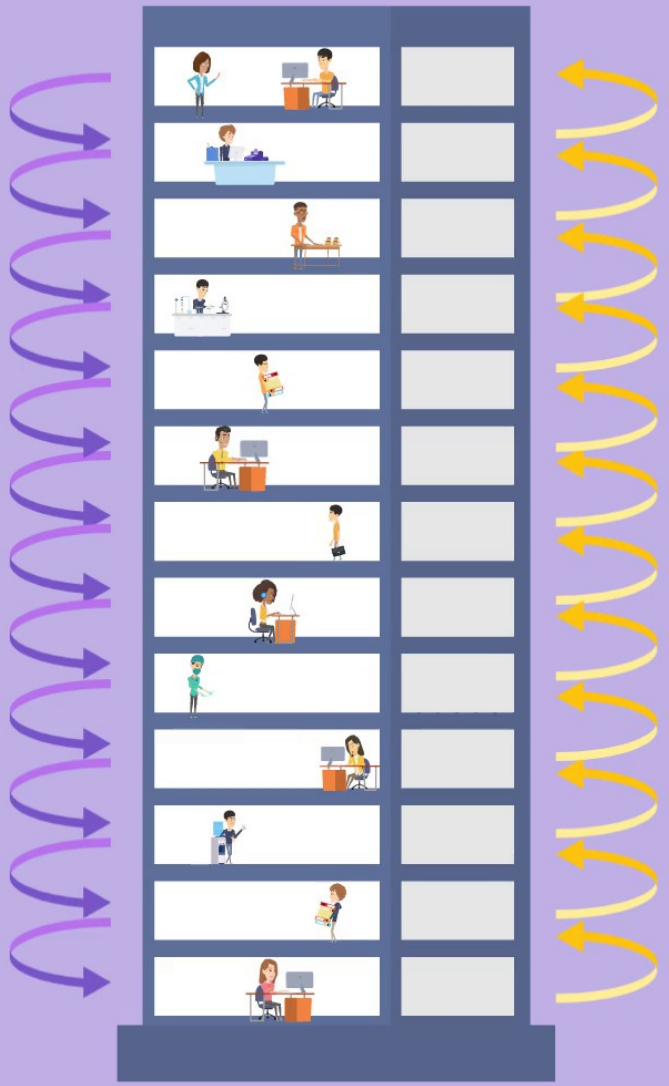
Product management

QA department

Software development

Open Source needs *both* ways

- The comany must be aware that Open Source is used.
- Compliance processes must be established.



Management

Strategic management

Research and Development

Product management

QA department

Software development

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*

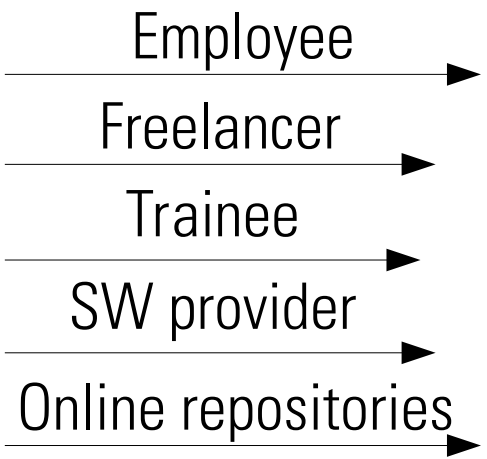
- Text blocks to modify contracts and other documents
- *Placeholders to be filled out individually*

→ Annexes providing processes and forms for legal information on products

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

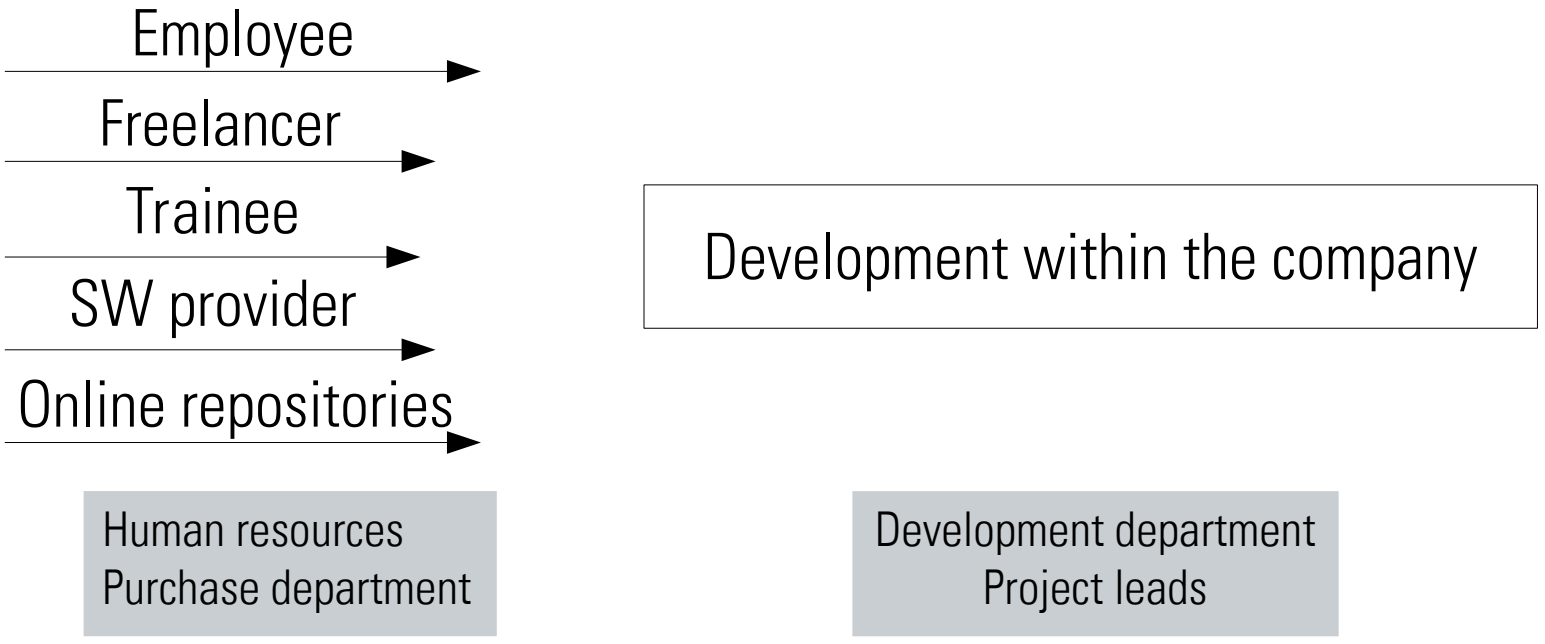
Software flow in a company

Software flow: Incoming software



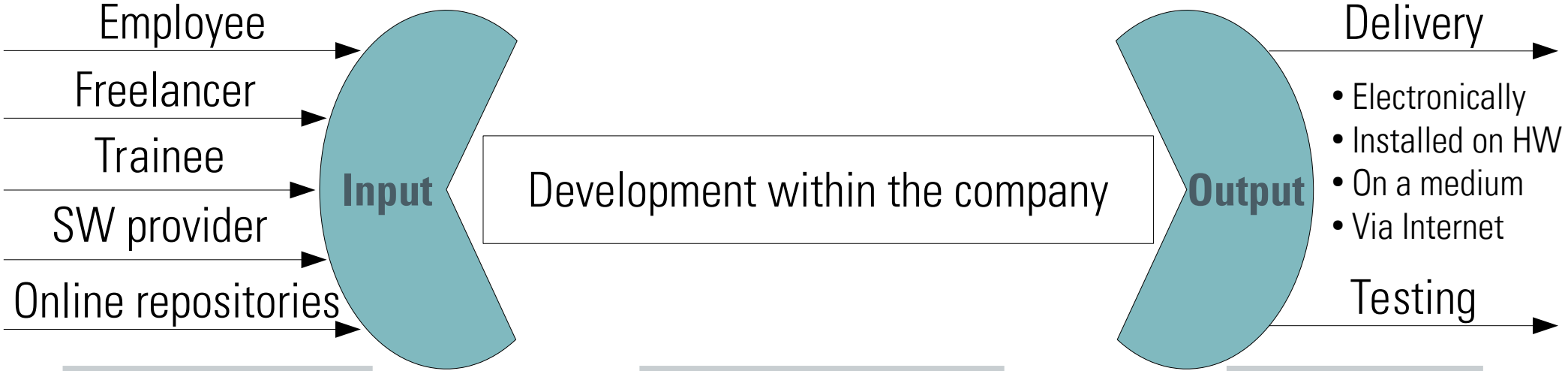
Human resources
Purchase department

Software flow: Own development



Software flow: Outgoing software

Software flow: Input/output gateways



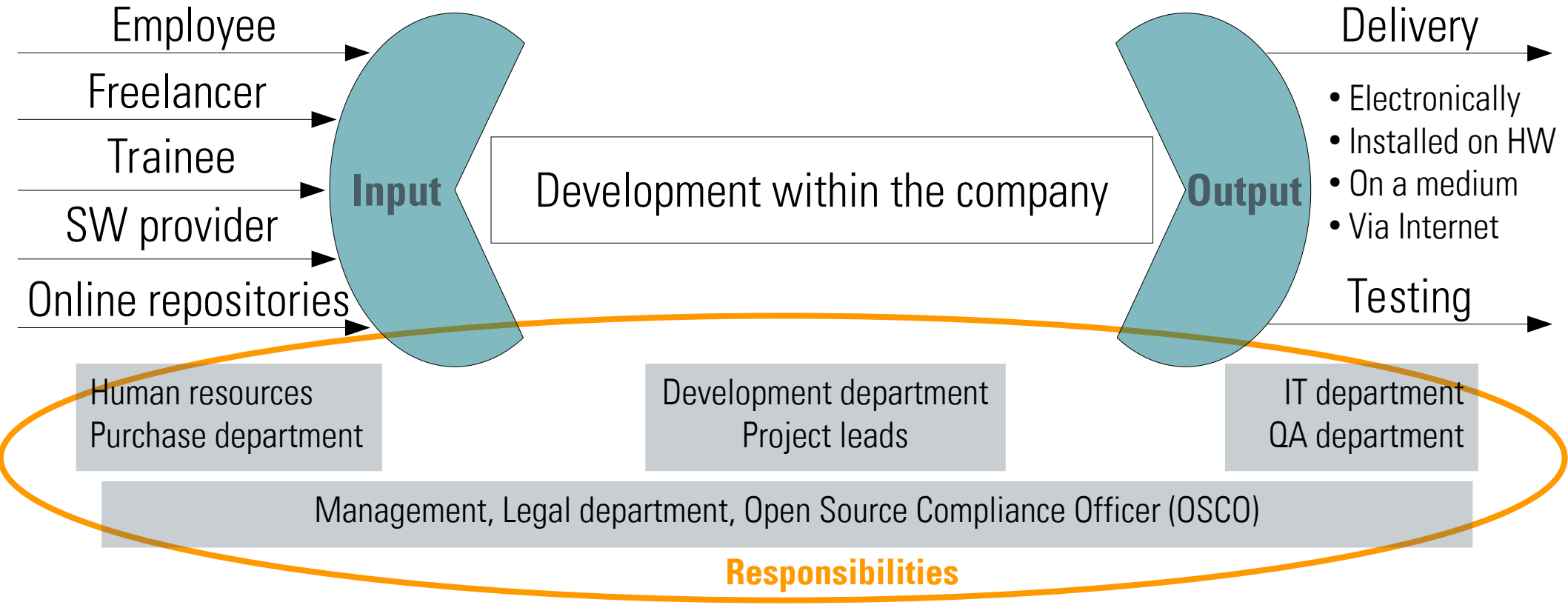
Human resources
Purchase department

Development department
Project leads

IT department
QA department

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

Software flow: Responsibilities

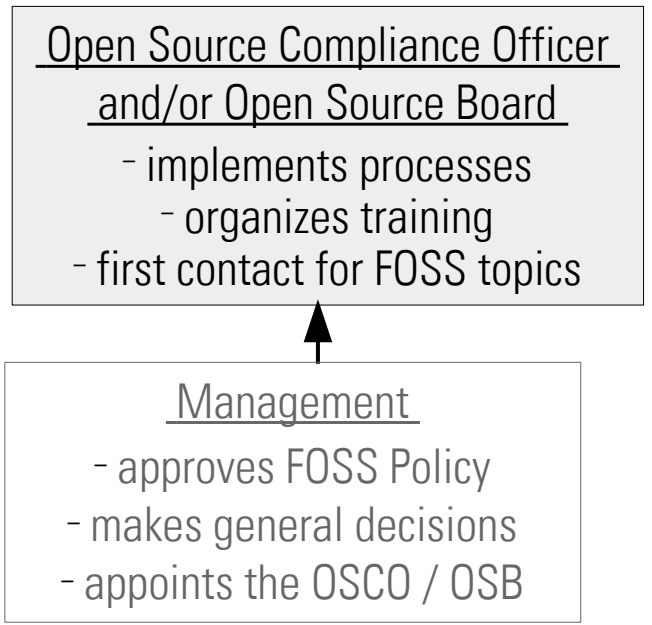


Responsibilities

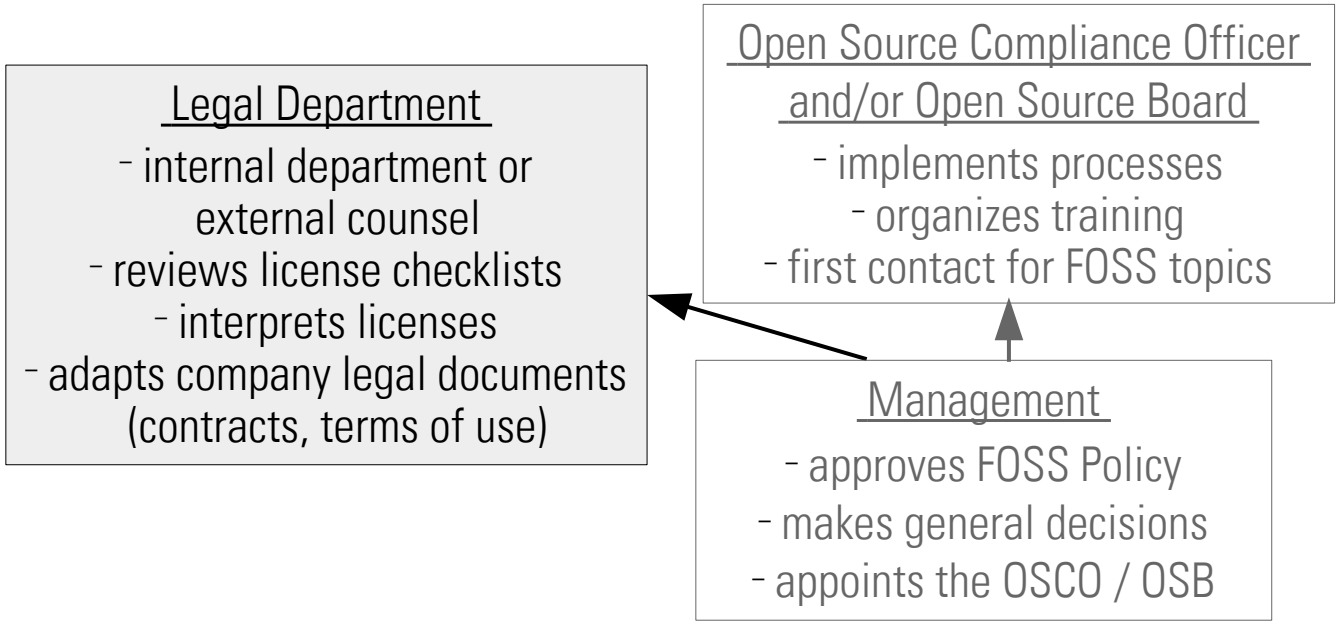
Management

- approves FOSS Policy
- makes general decisions
- appoints the OSCO / OSB

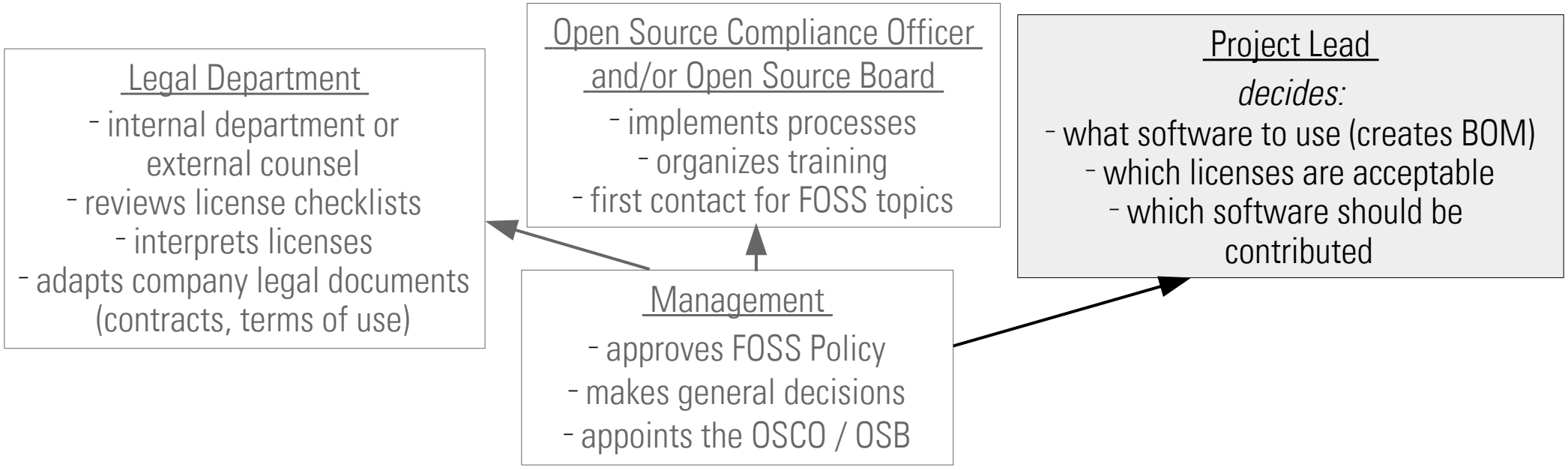
Responsibilities



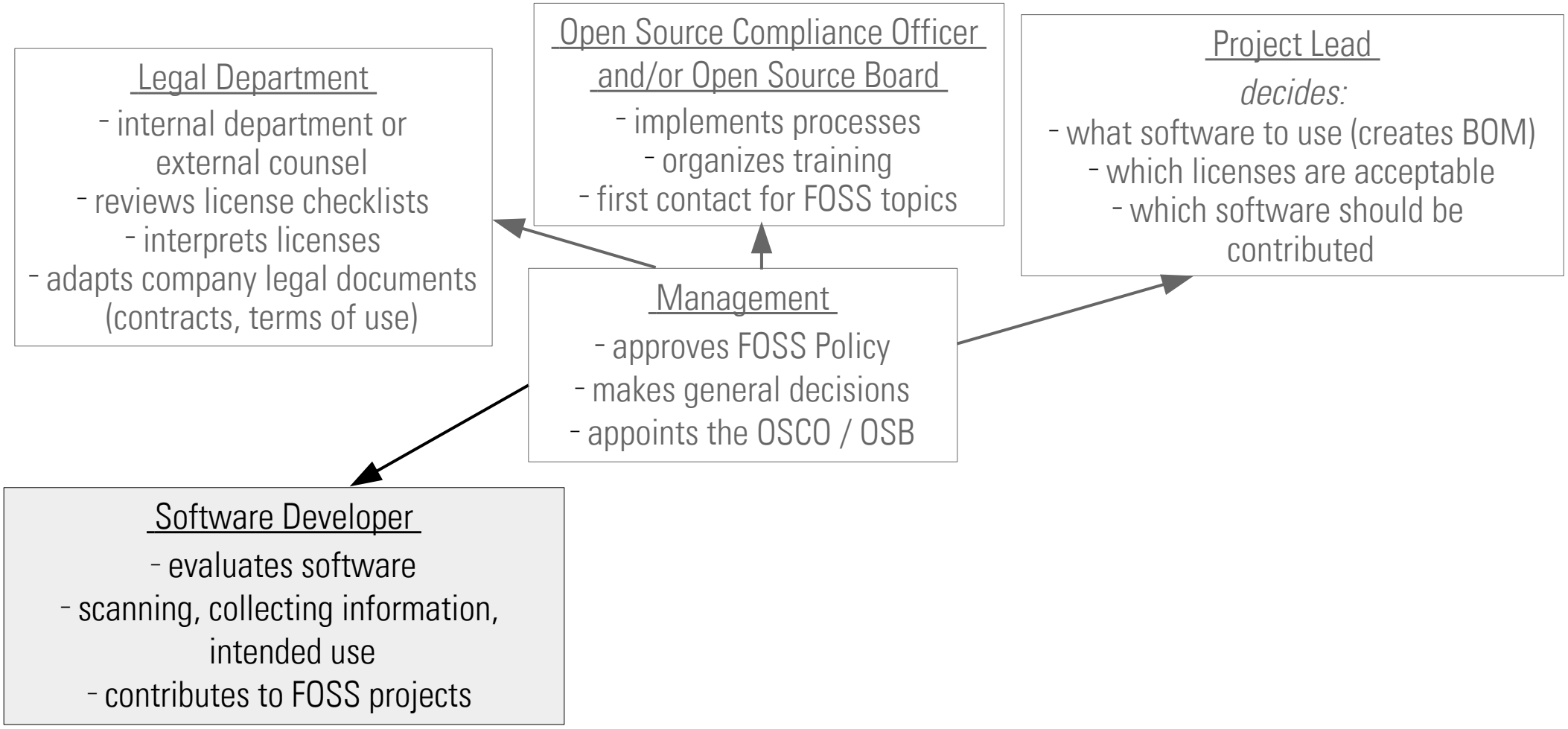
Responsibilities



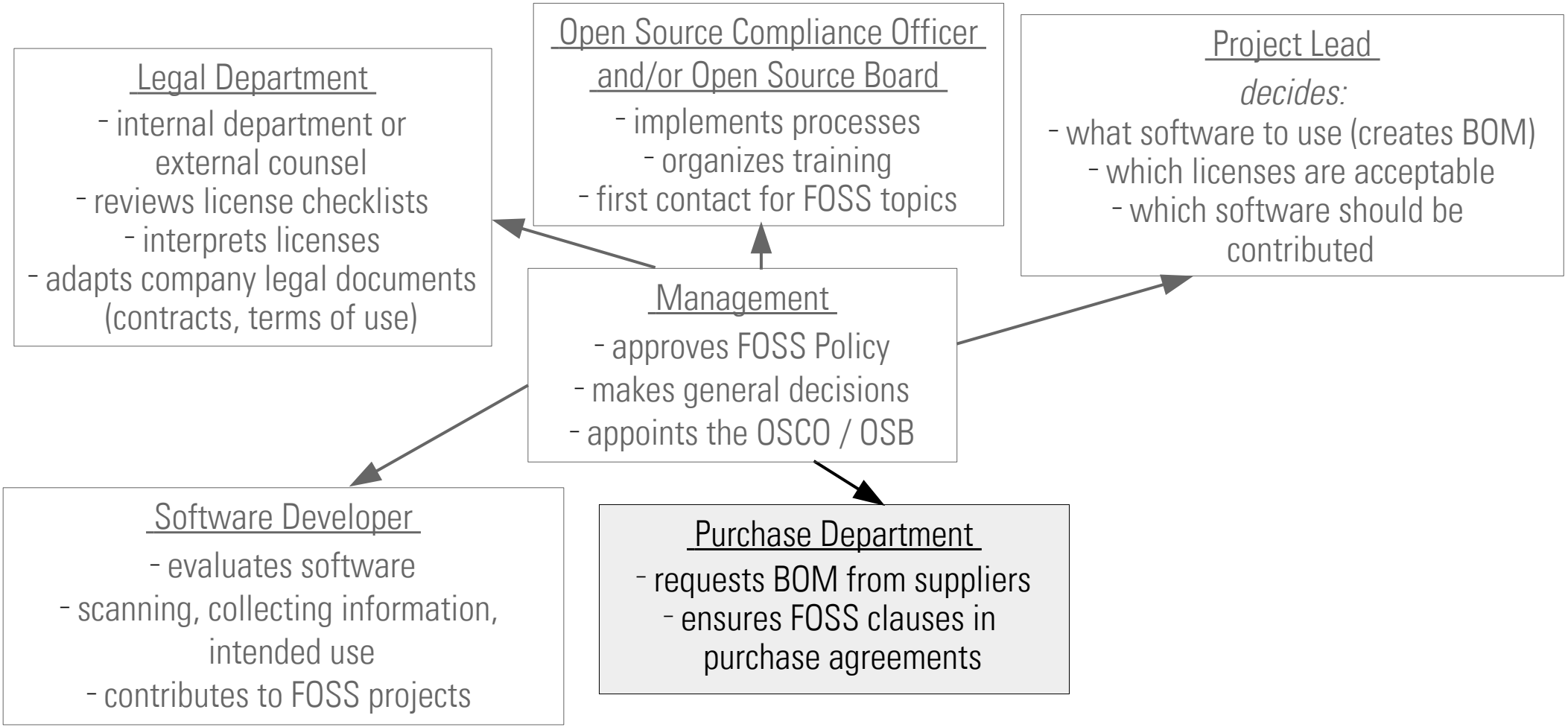
Responsibilities



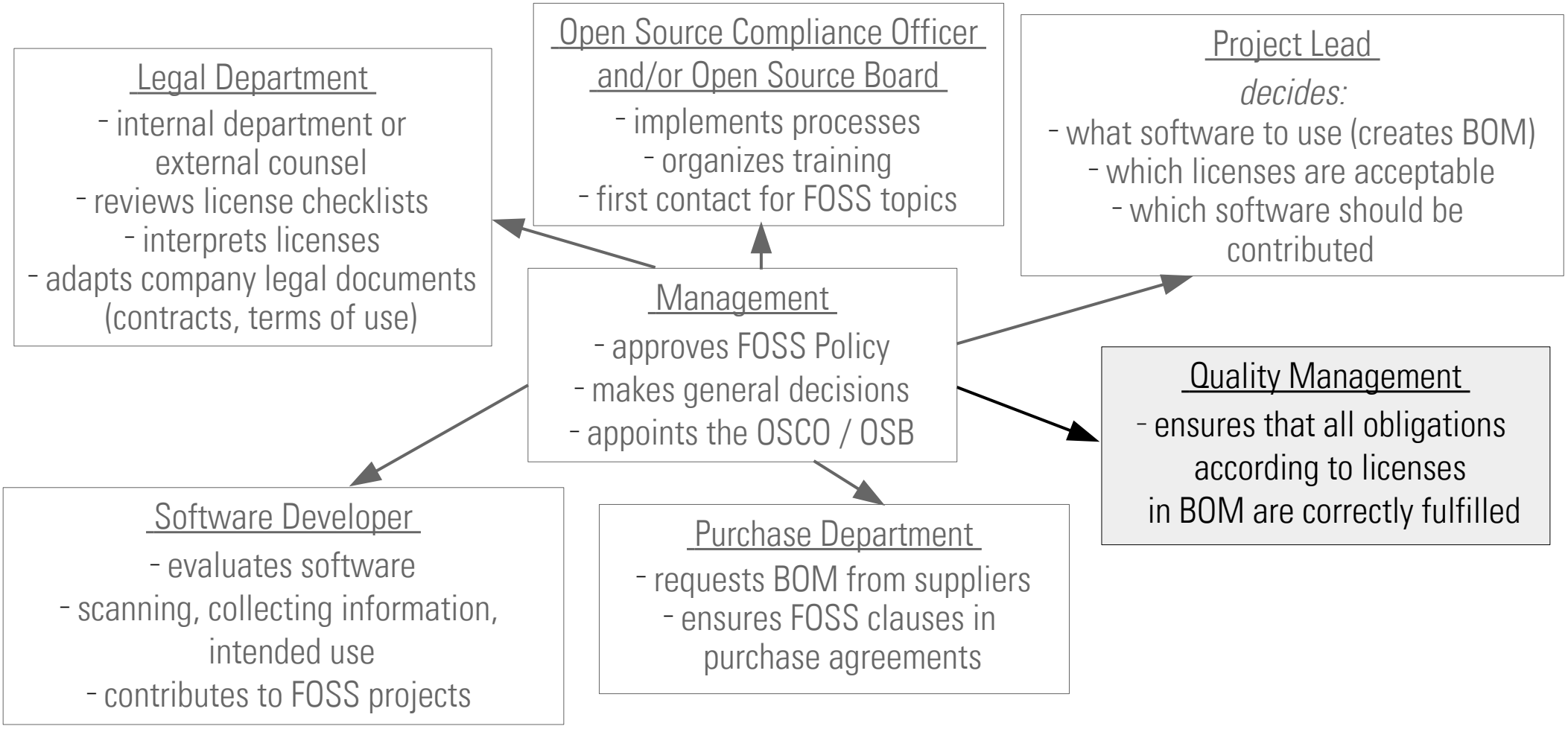
Responsibilities



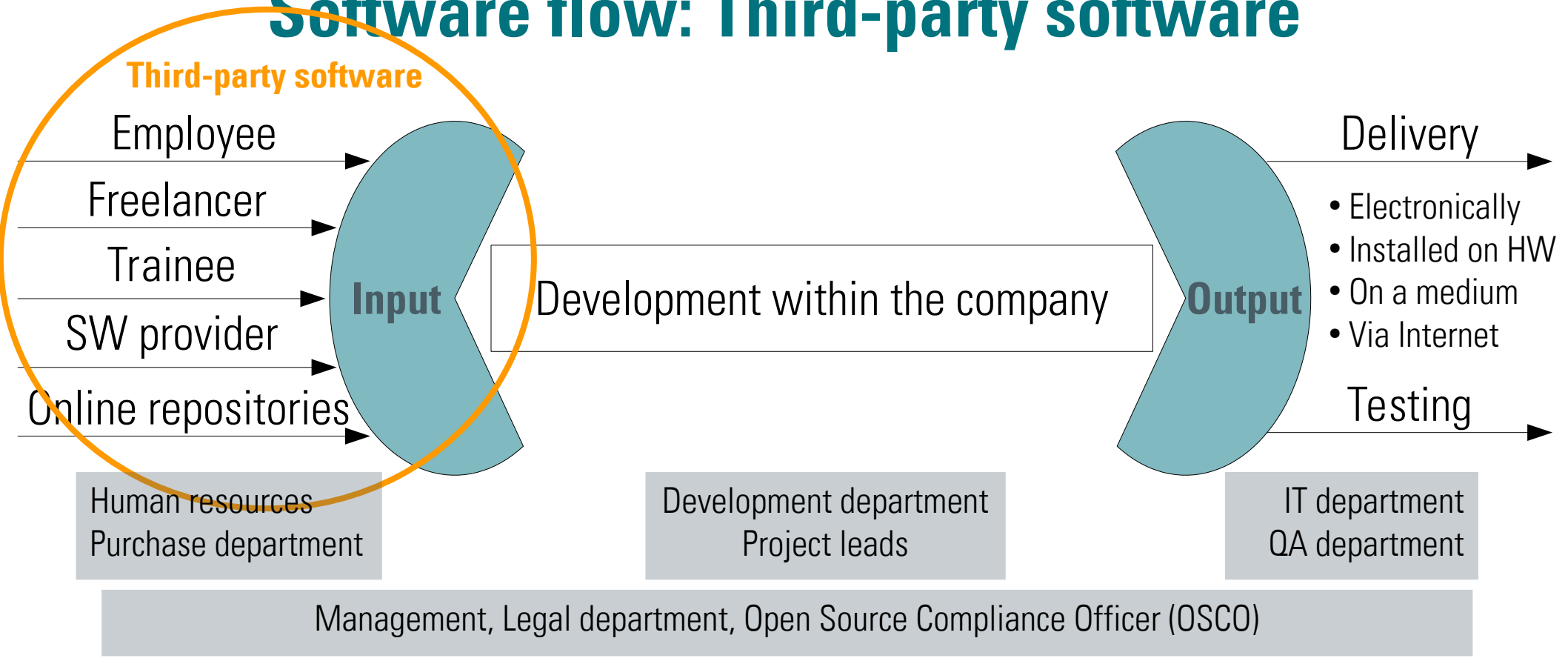
Responsibilities



Responsibilities



Software flow: Third-party software



Detection and analysis of third-party software (1)

Goals

- Control over what external software is used
- Avoiding unlicensed software
- Basis for creating a BOM (Bill of Material)

Detection and analysis of third-party software (2)

- ***Option 1: No rules apply to in-house FOSS***
  - FOSS may be used within a legal entity without restrictions or obligations.
  - Exempting in-house FOSS from approval processes reduces expenses.
- ***Option 2: All FOSS is treated as equal***
  - Identical processes are established for in-house FOSS and distributed FOSS.
  - This takes into account future mergers and acquisitions or changes from internal use to distribution.

Detection and analysis of third-party software (3)

Evaluation of technical suitability

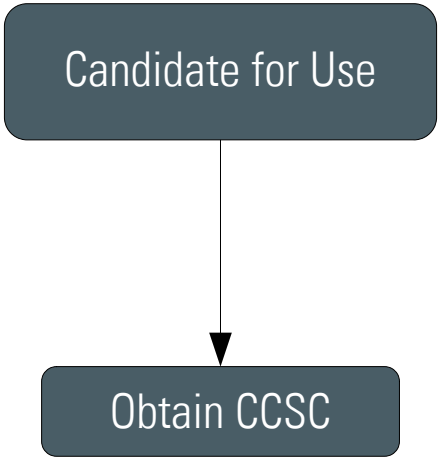
- Freely downloadable software may be evaluated.
- If license agreements or terms of use need to be accepted, a request to the legal department must be submitted.
- Name of the software, download link, legal text

Checking software into internal repositories is only allowed with prior approval according to the process outlined in this policy.

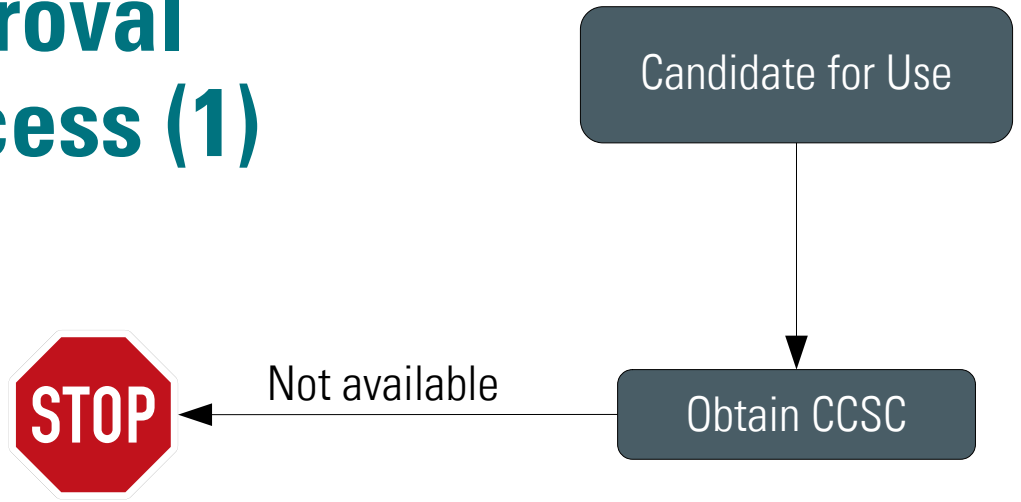
→ **Annex: Approval process**

Approval process (1)

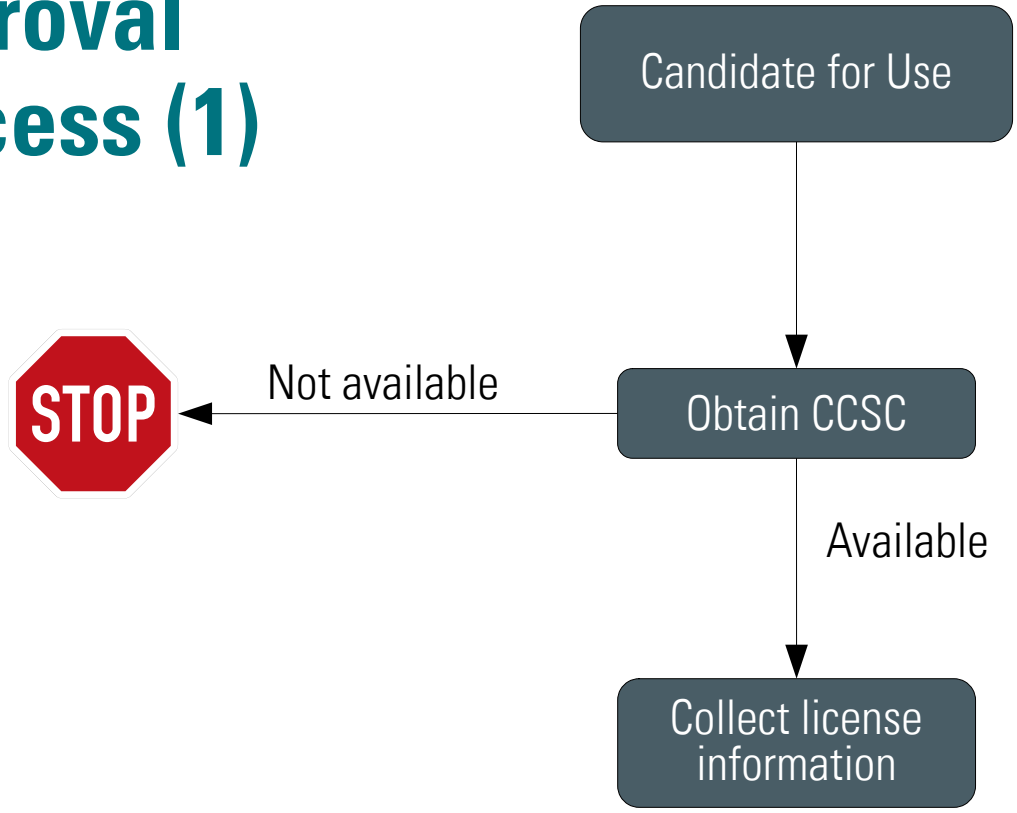
Approval process (1)



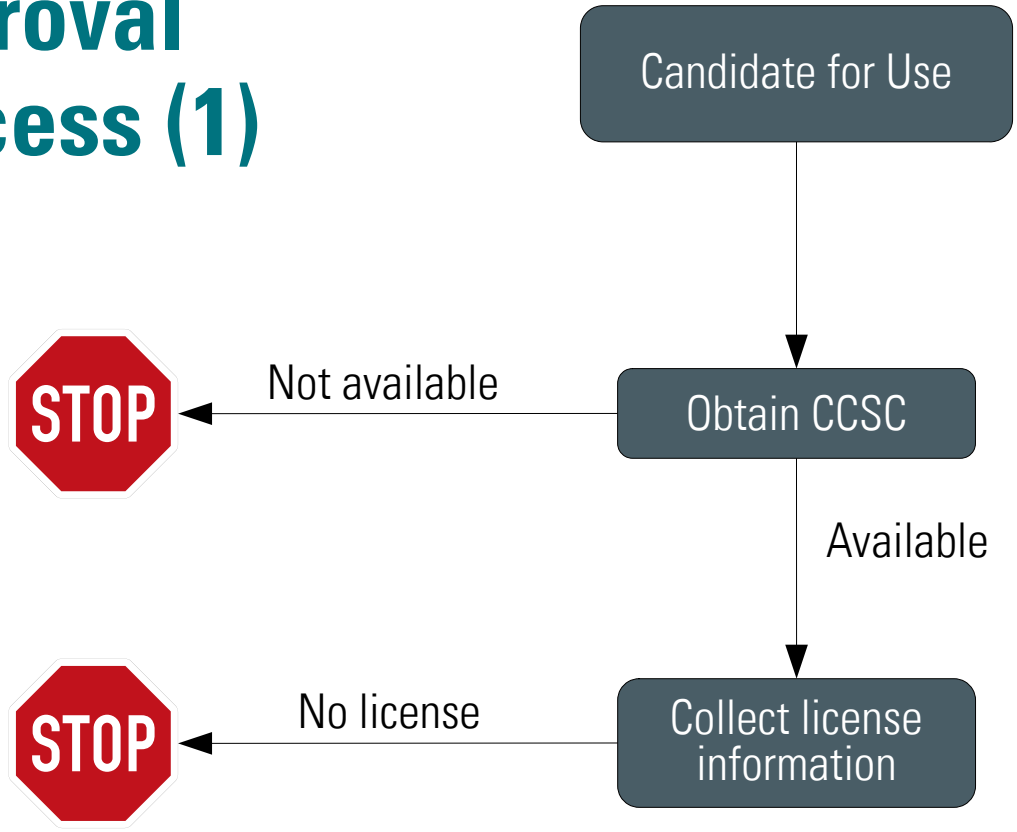
Approval process (1)



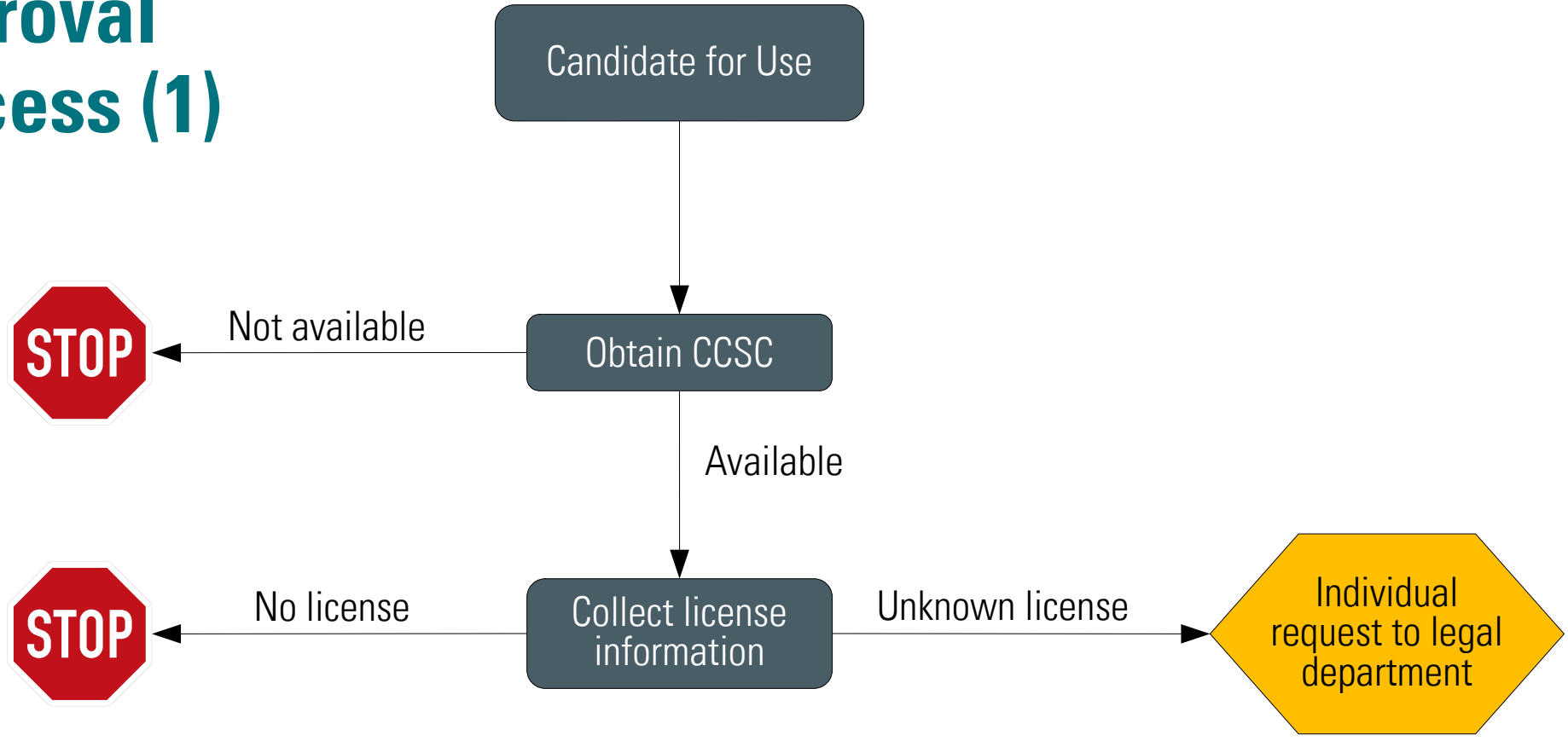
Approval process (1)



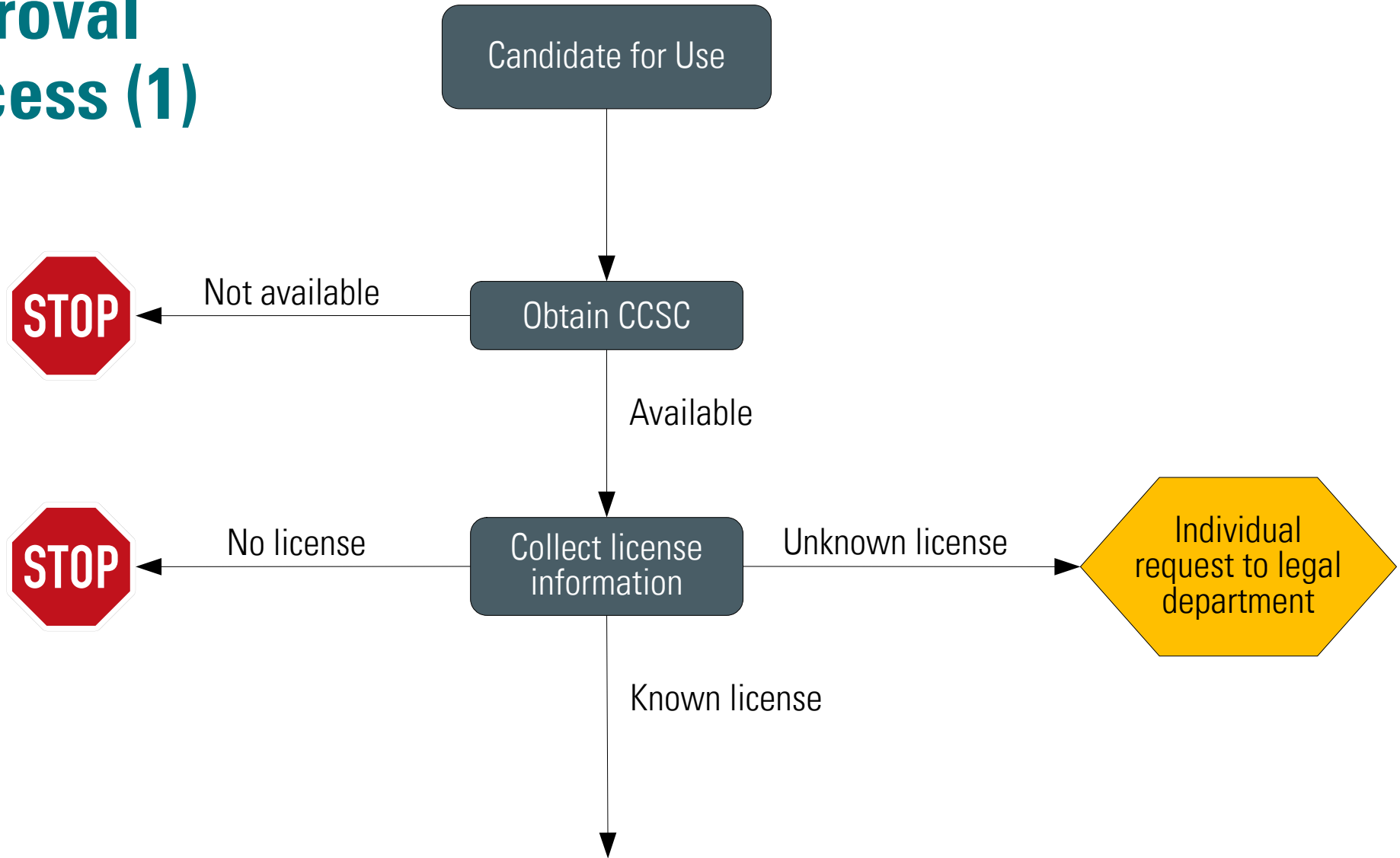
Approval process (1)



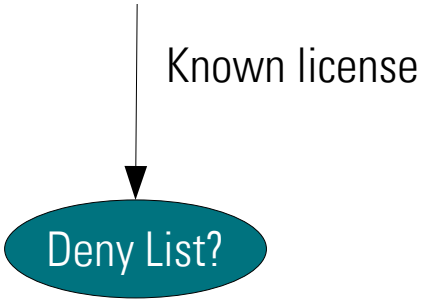
Approval process (1)



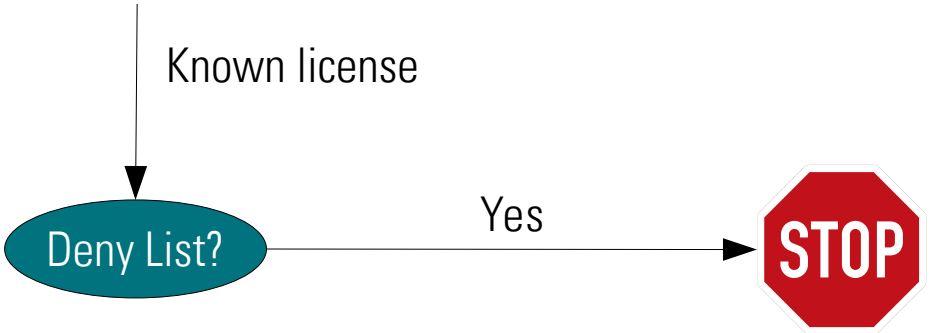
Approval process (1)



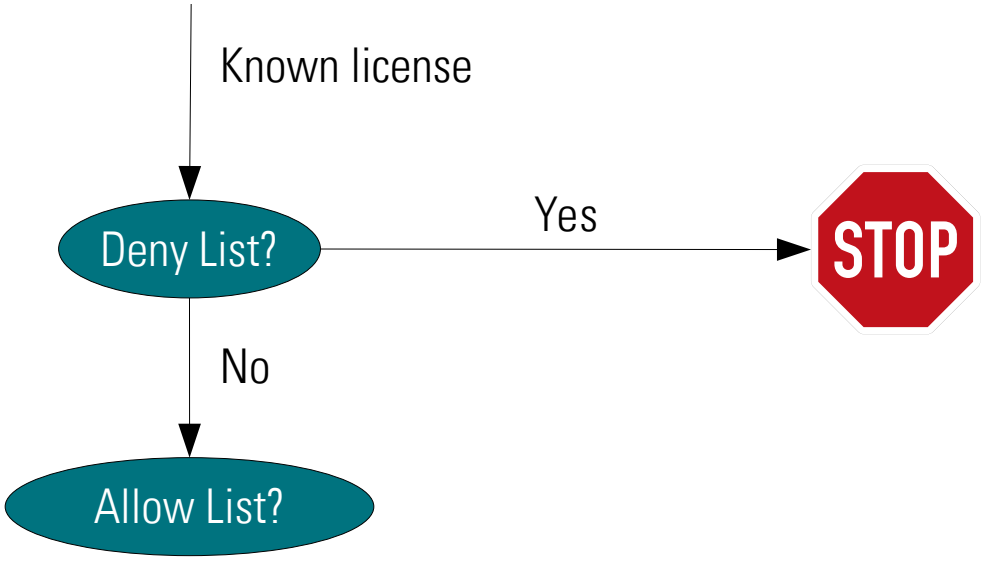
Approval process (2)



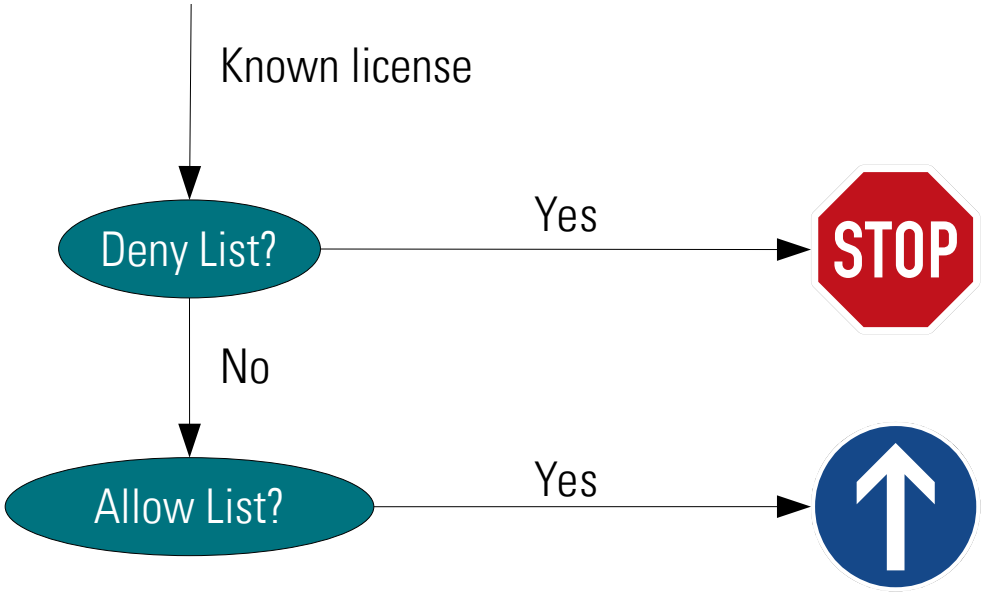
Approval process (2)



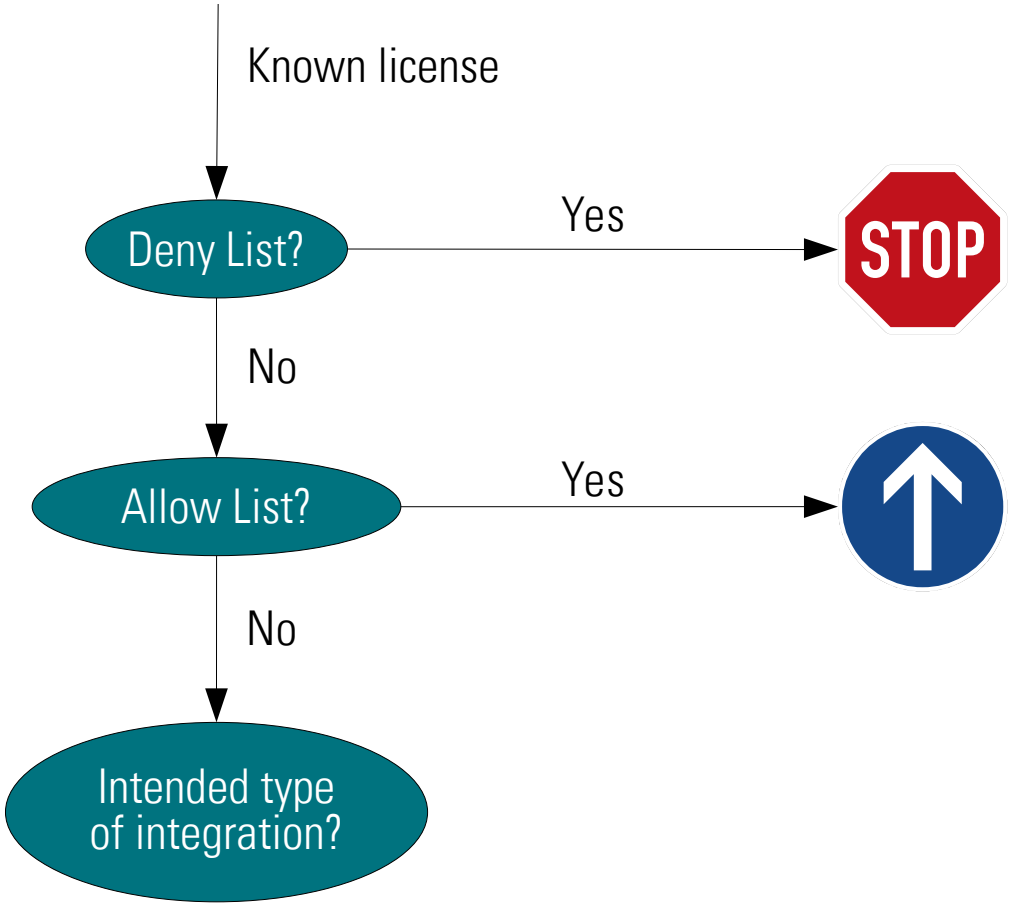
Approval process (2)



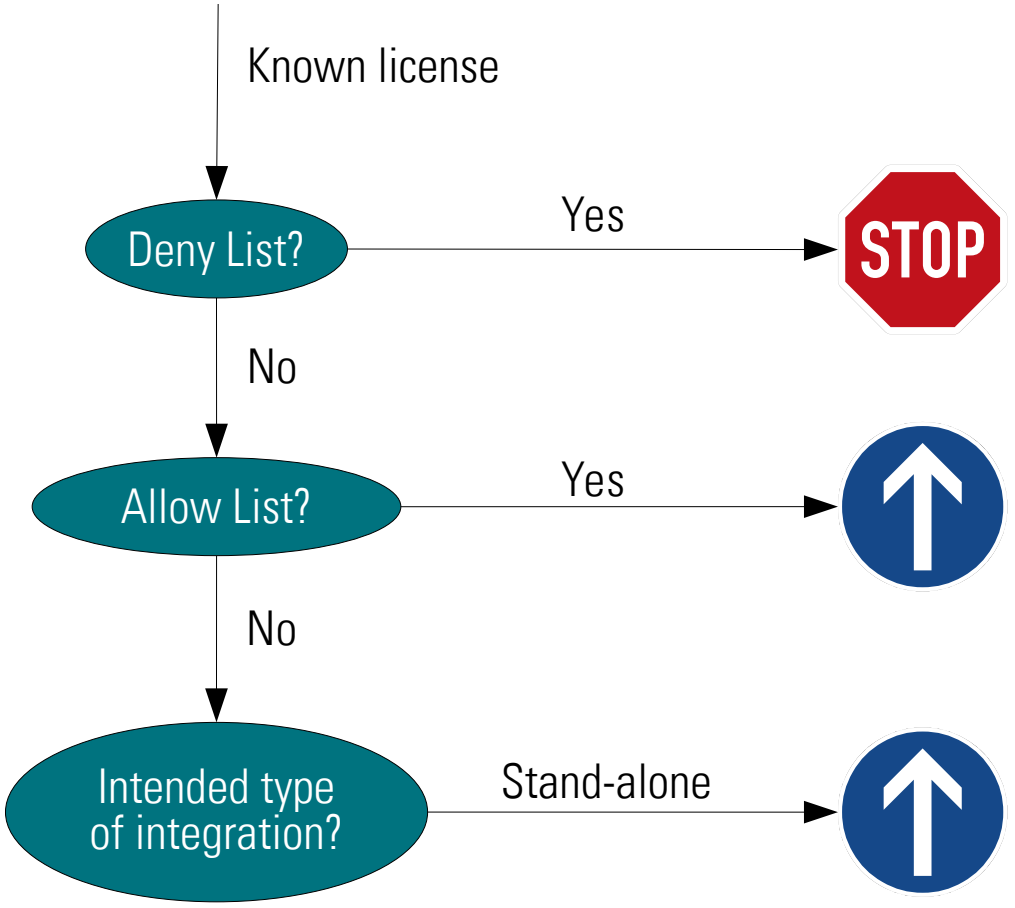
Approval process (2)



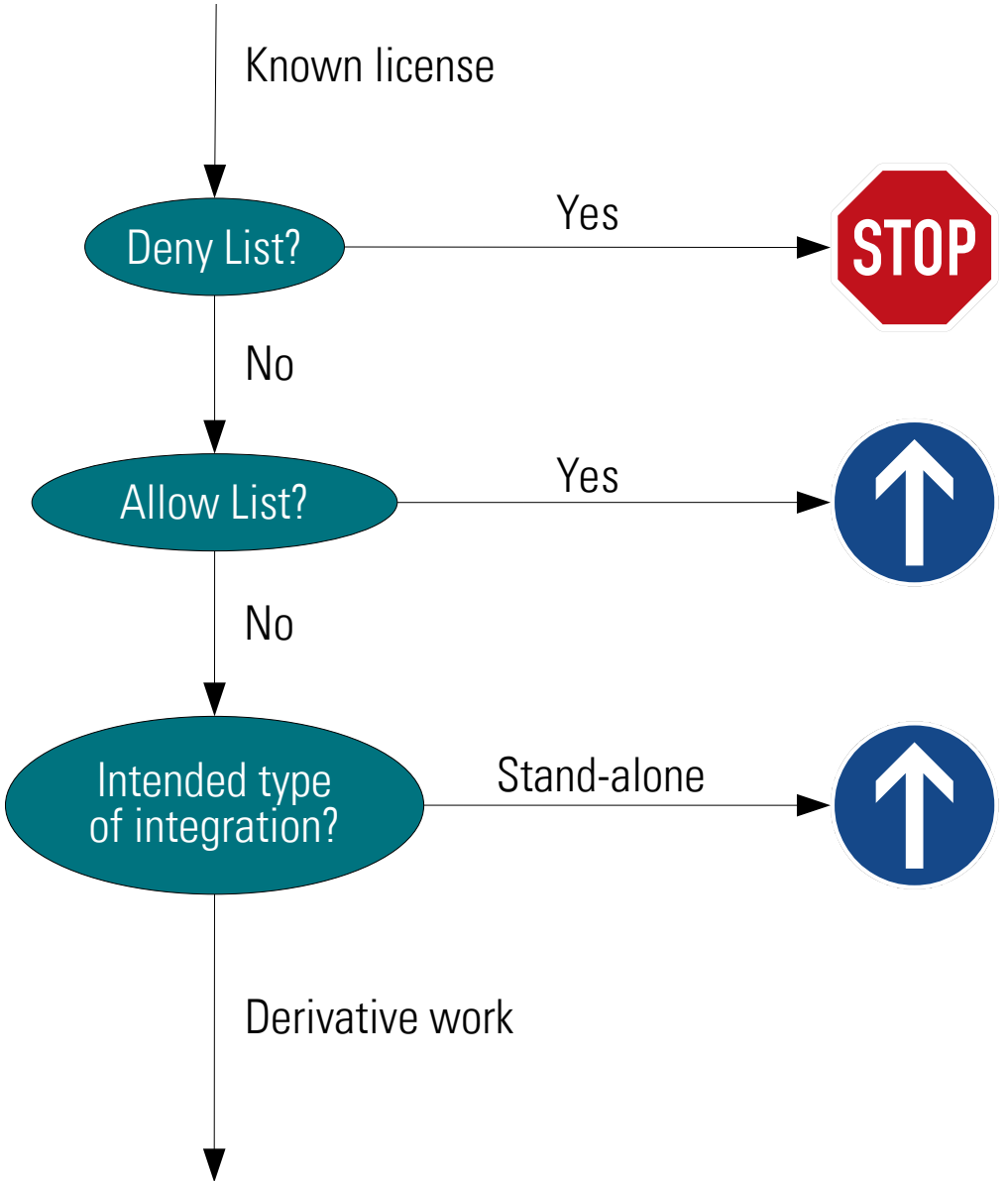
Approval process (2)



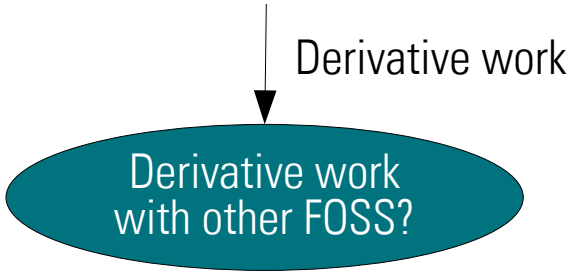
Approval process (2)



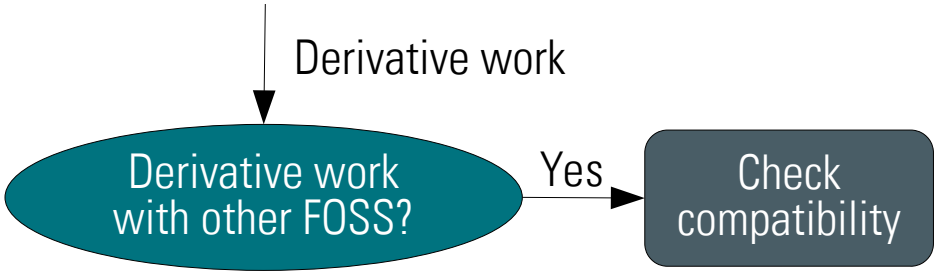
Approval process (2)



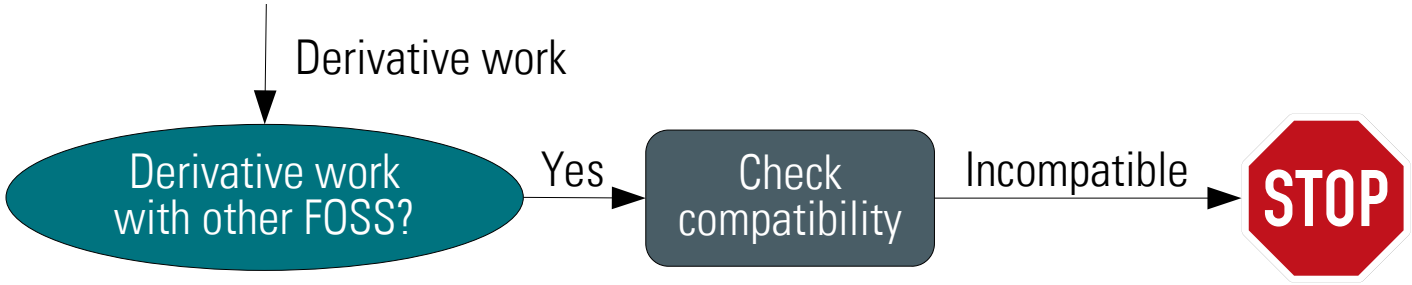
Approval process (3)



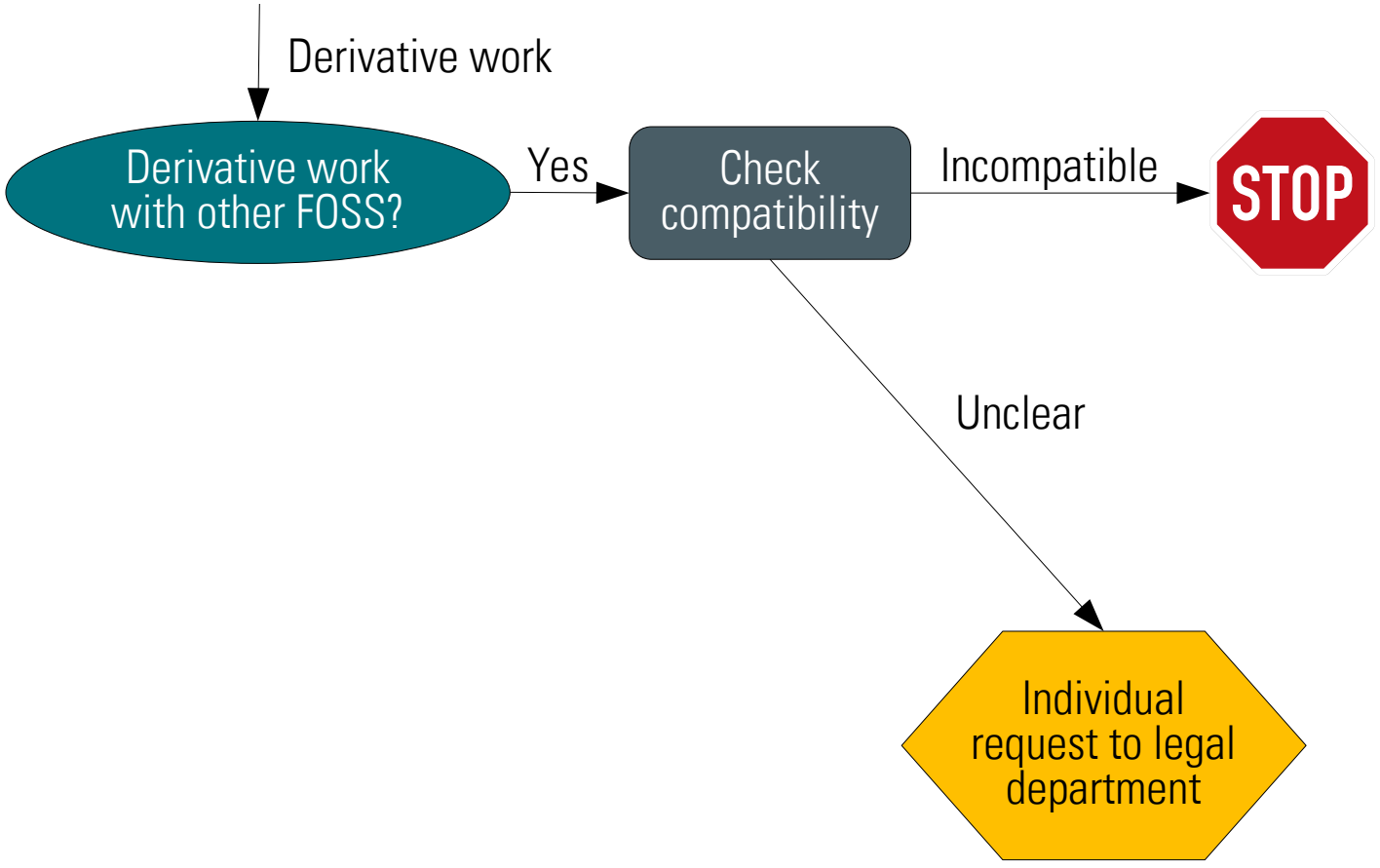
Approval process (3)



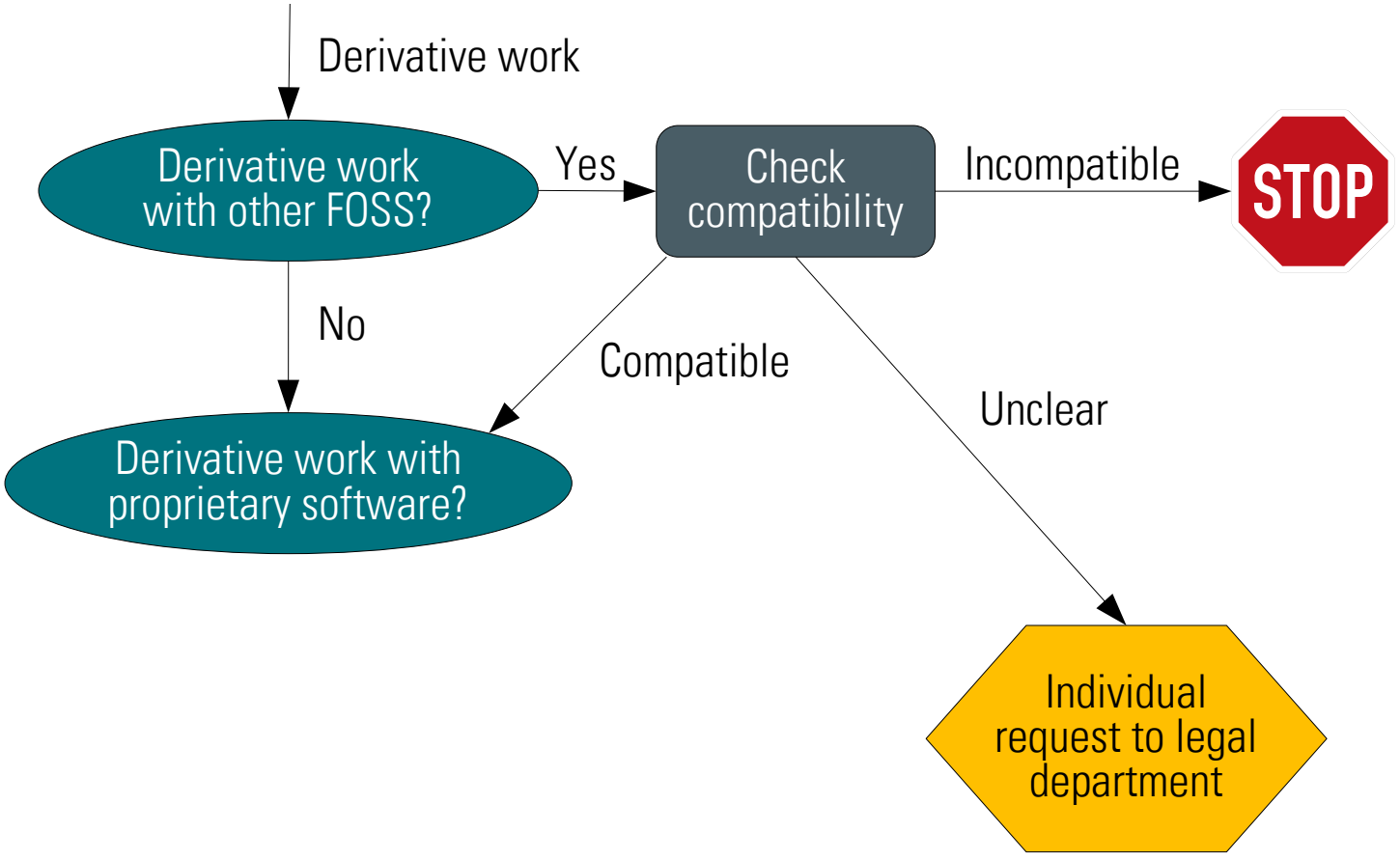
Approval process (3)



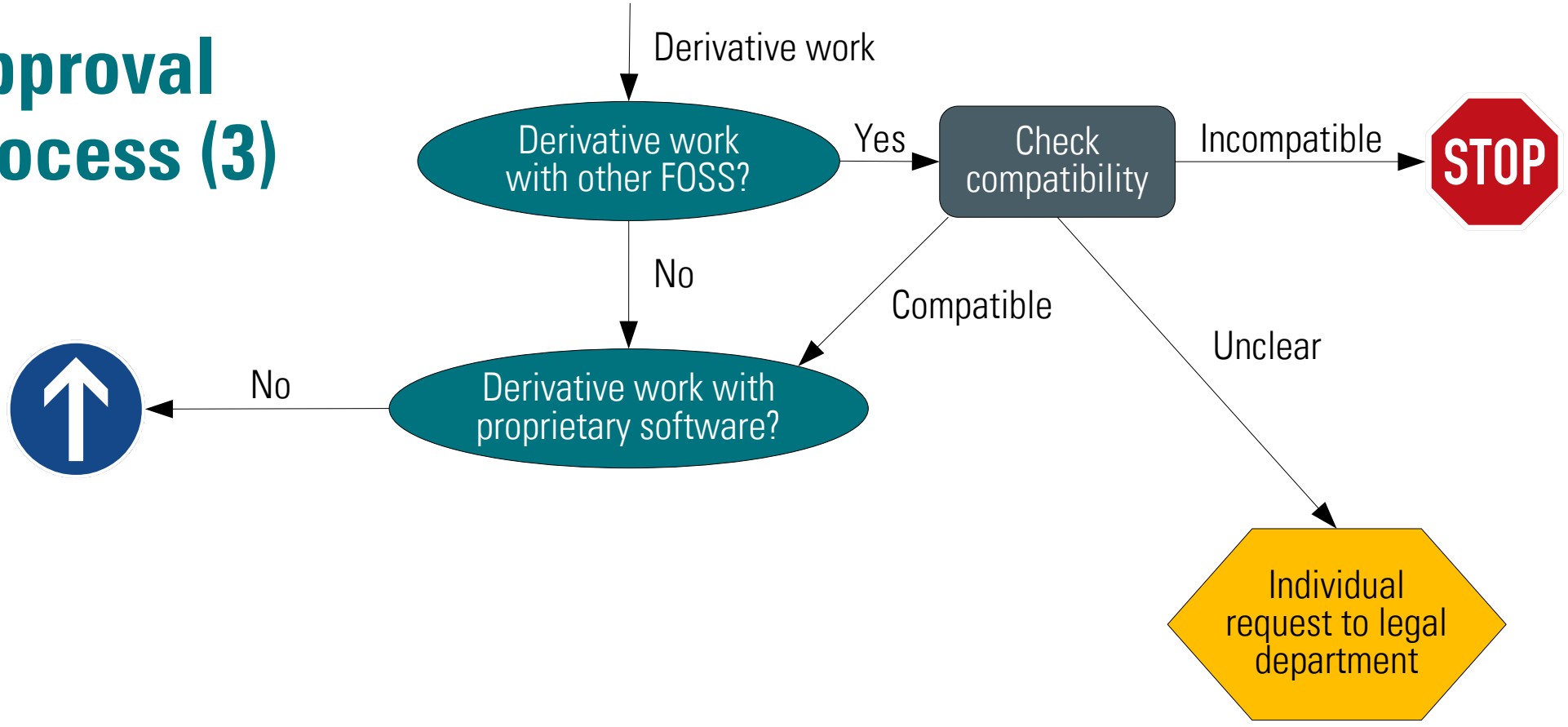
Approval process (3)



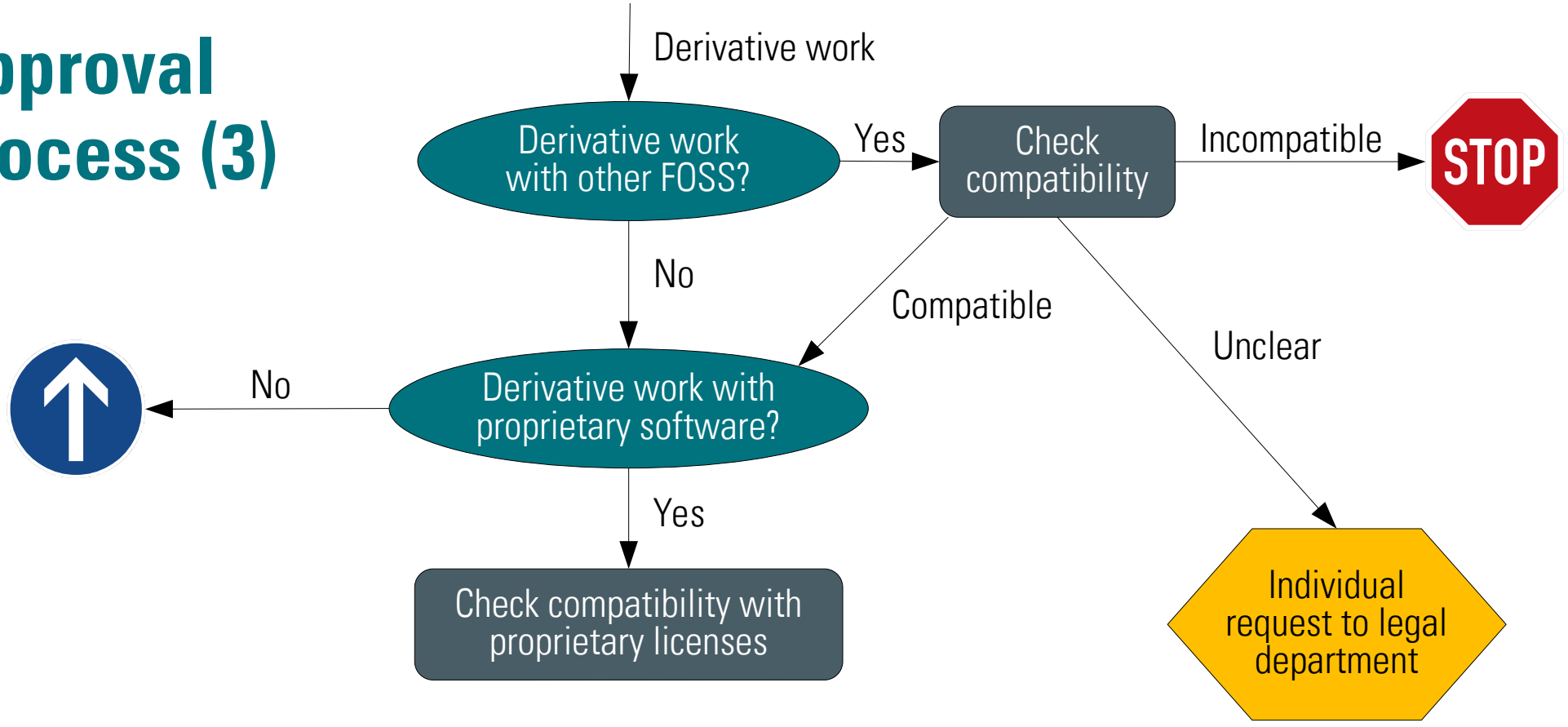
Approval process (3)



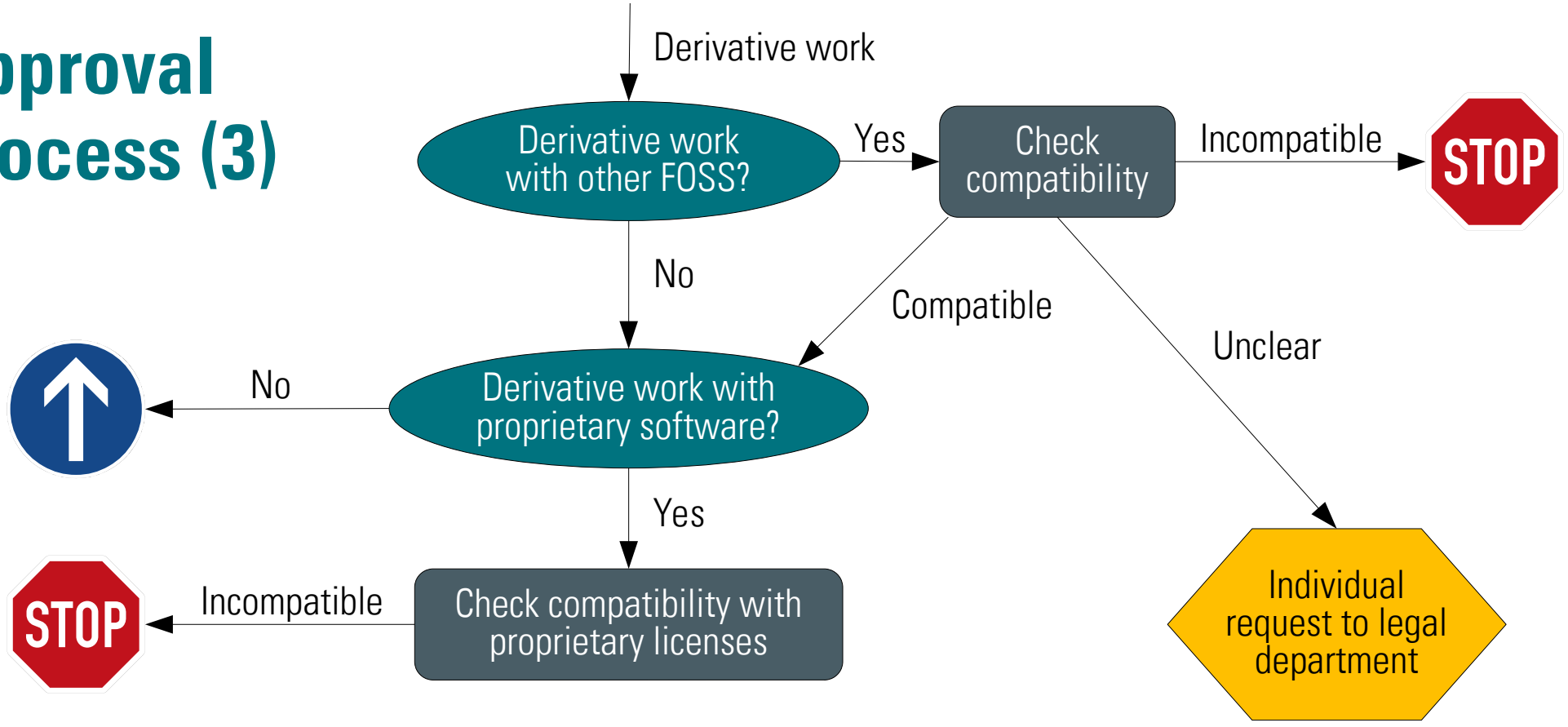
Approval process (3)



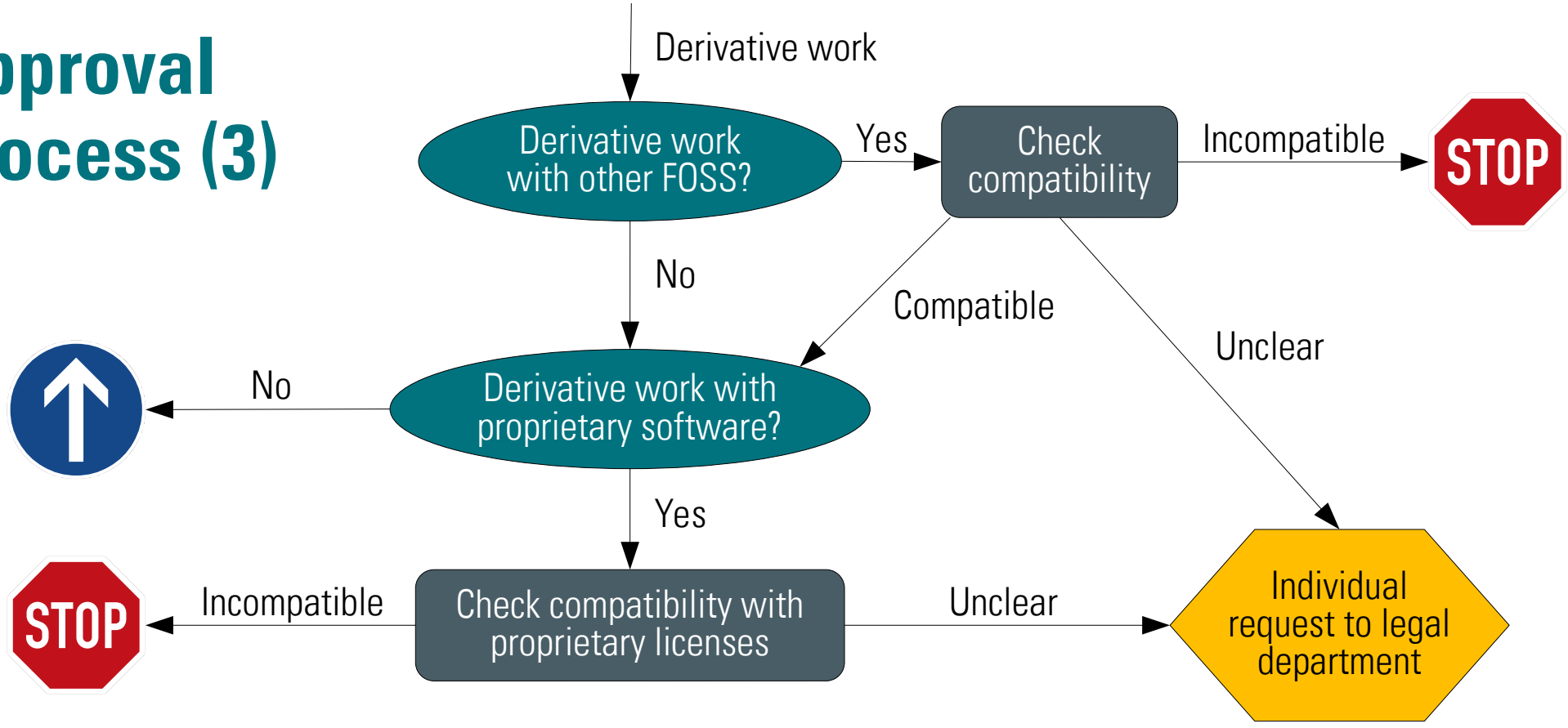
Approval process (3)



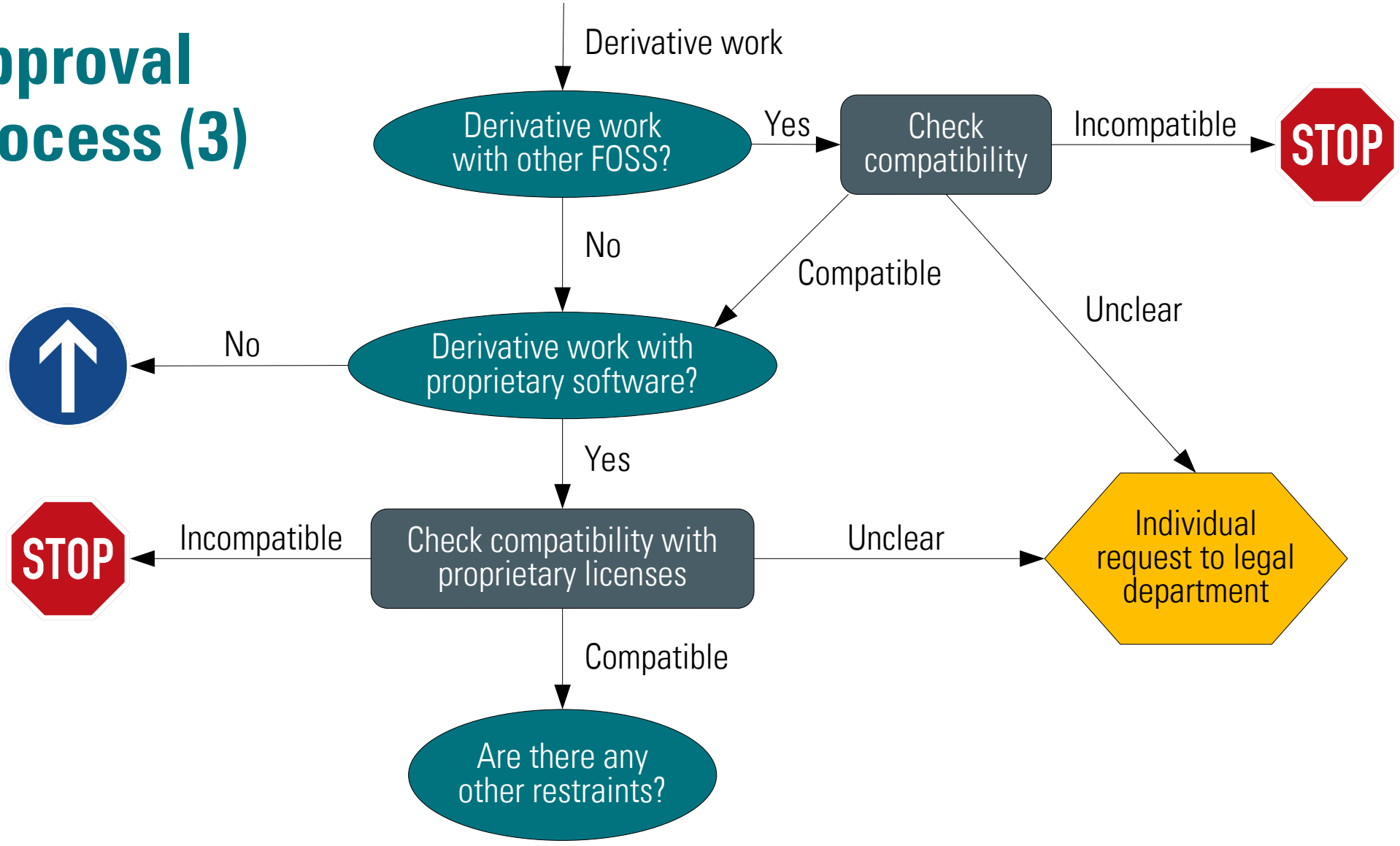
Approval process (3)



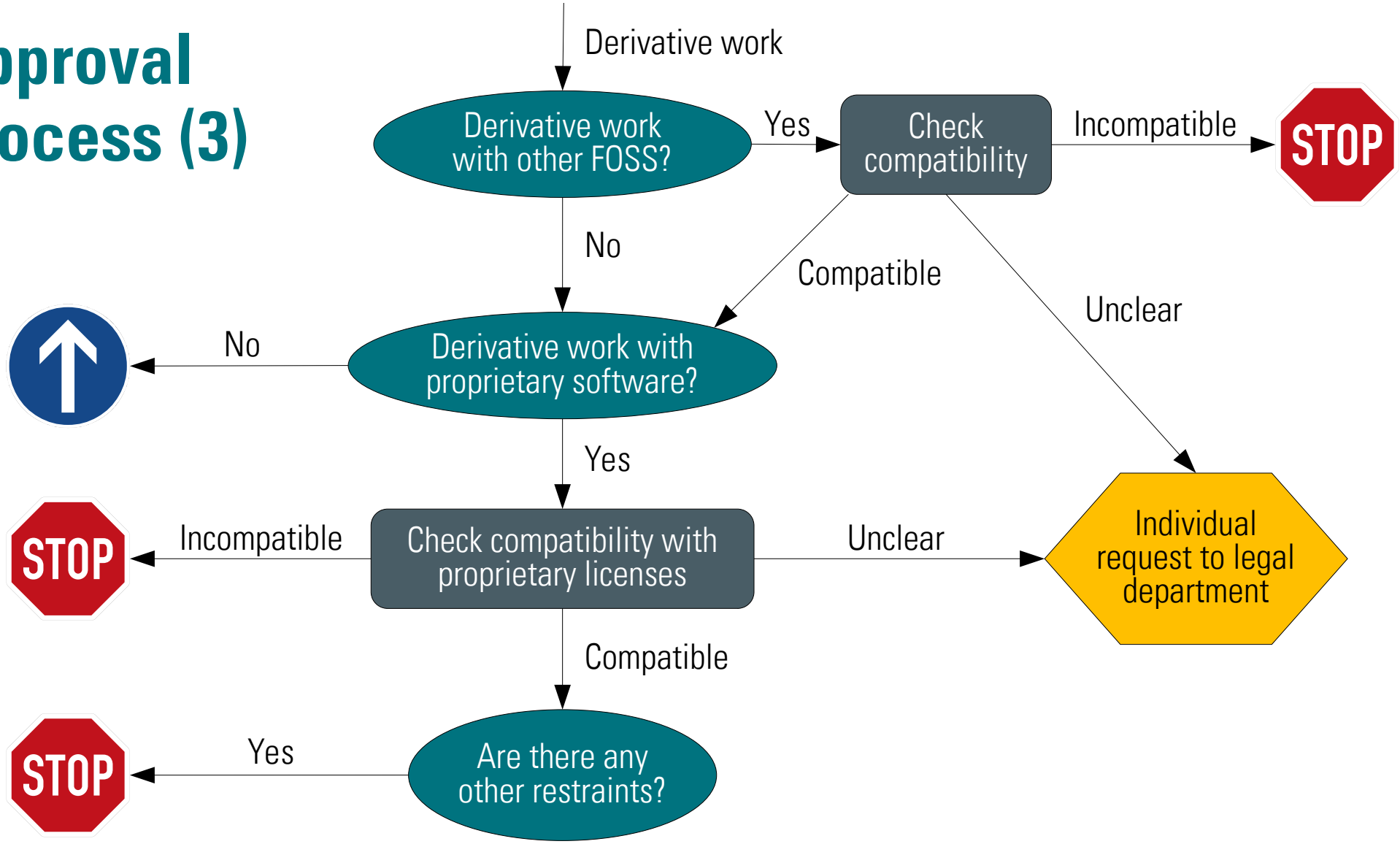
Approval process (3)



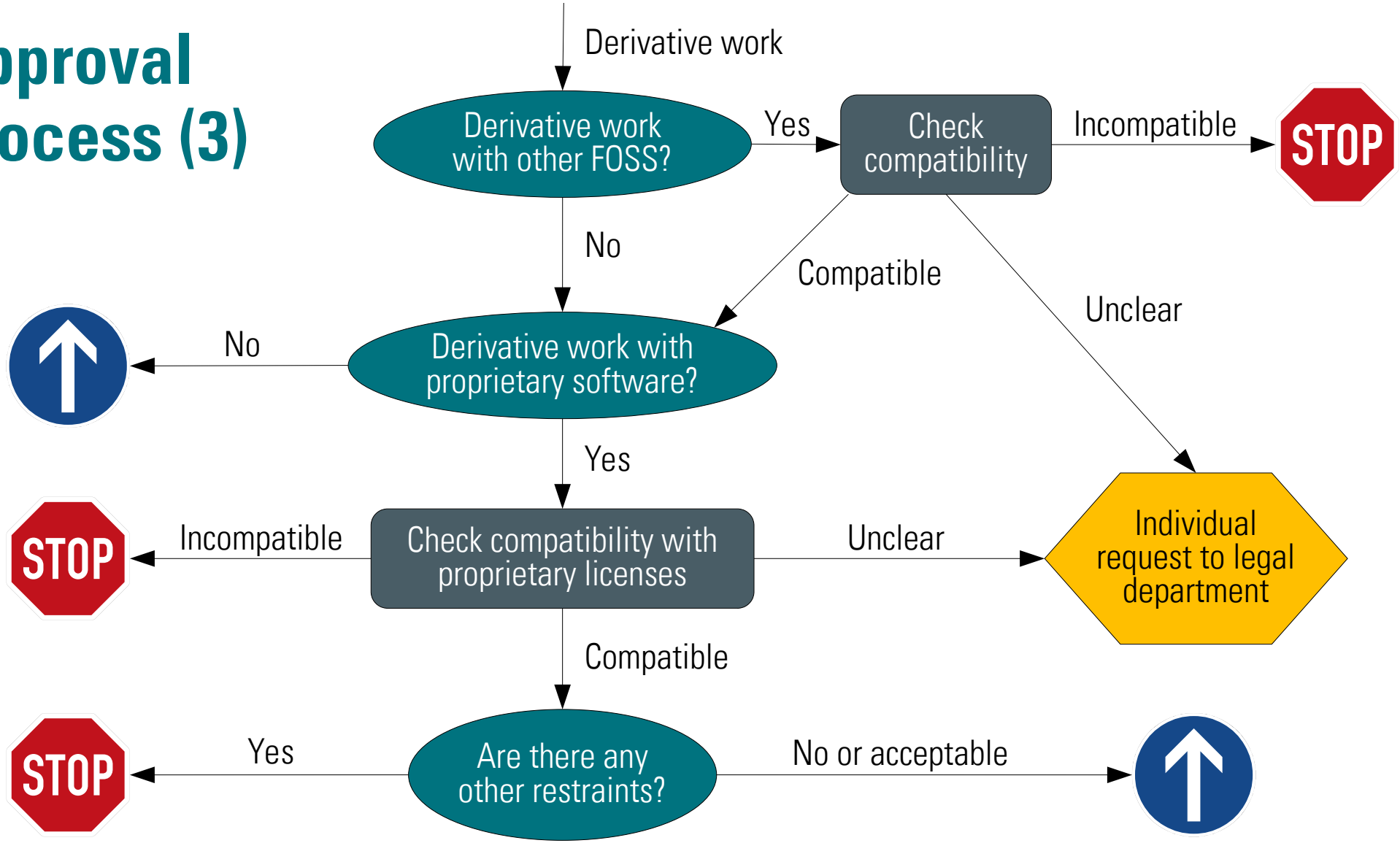
Approval process (3)



Approval process (3)



Approval process (3)



Approval process (4)

The software may be checked into the company repository with:

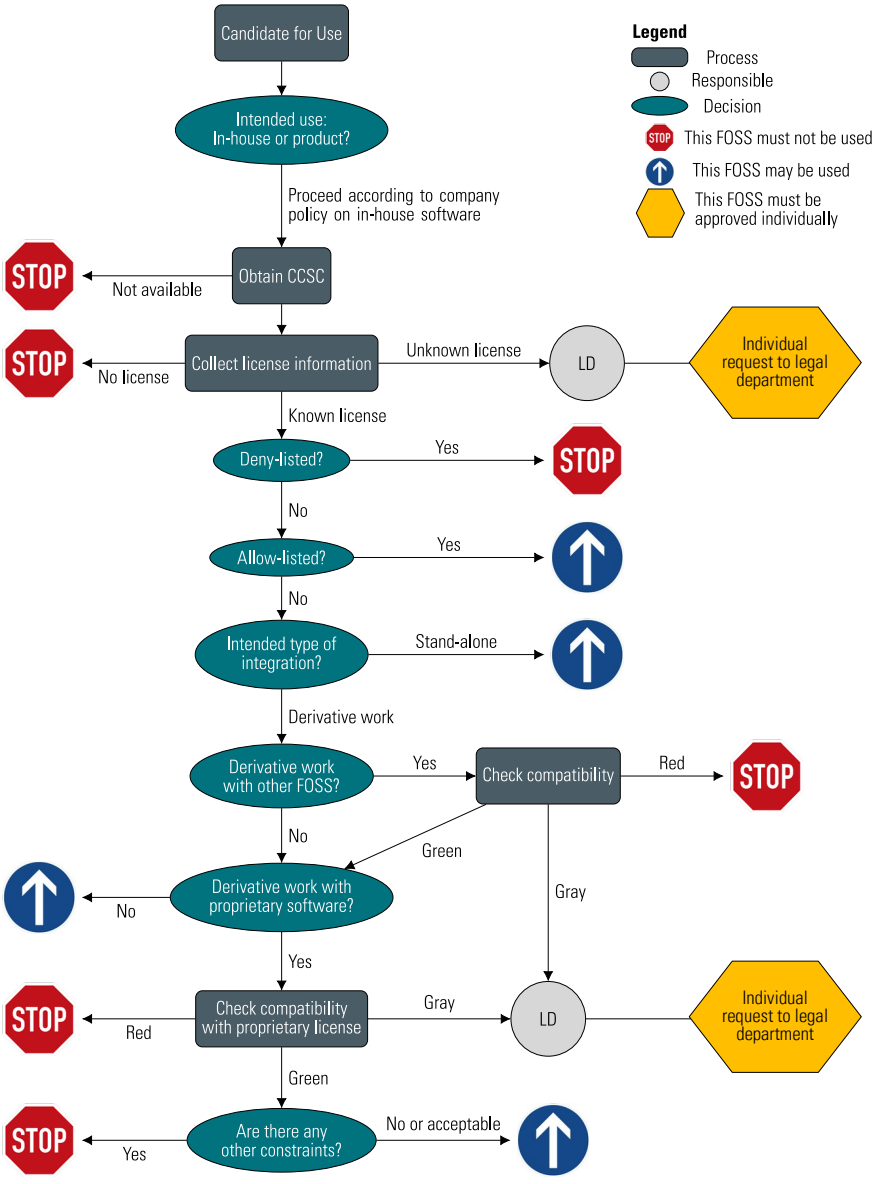
- Software name and version
- Complete Corresponding Source Code (CCSC)
- (Re)Build instructions
- legal information

The software component is not suitable for use in the company's products. This information must be archived and an alternative must be found.

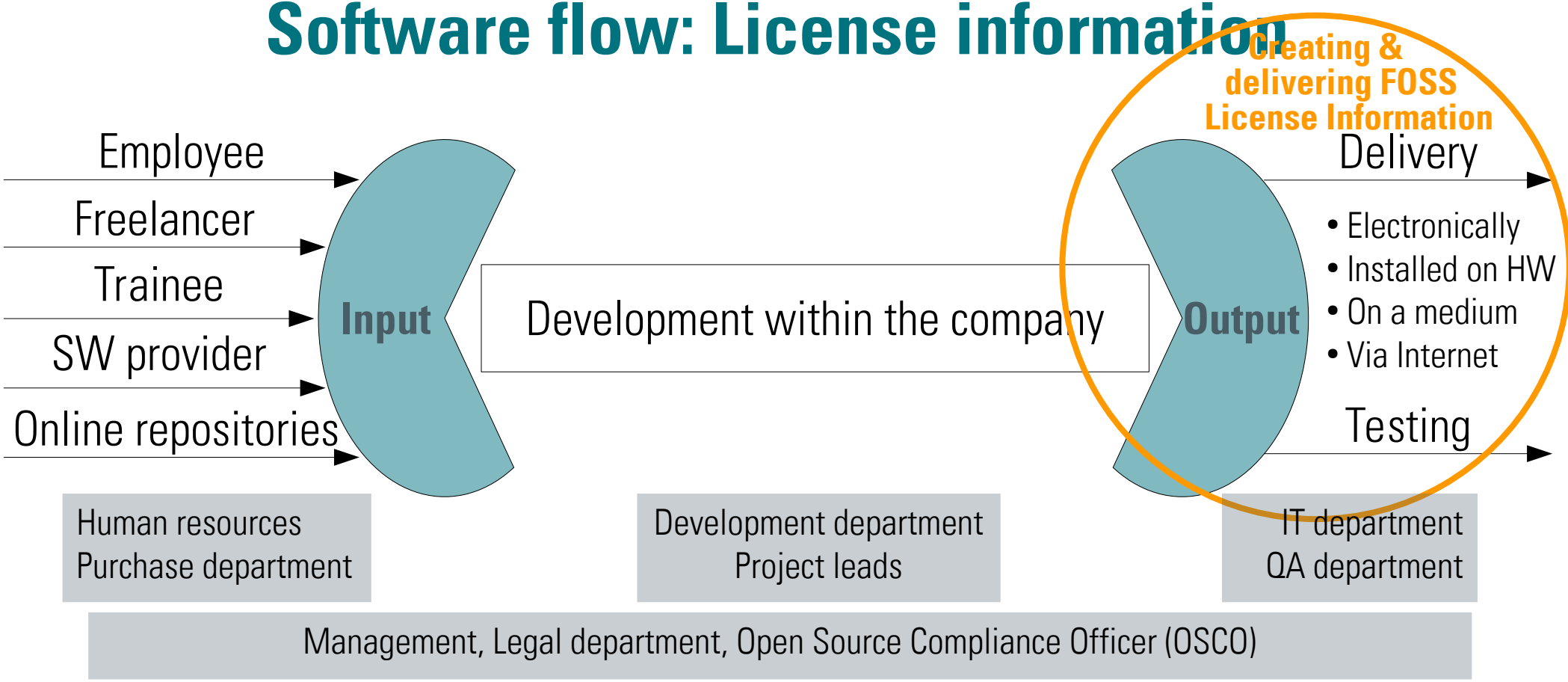
An individual request to the legal department must be submitted.

Approval process (5)

Reduces individual requests, if a software component is legally suitable for use (distribution) in a product



Software flow: License information



FOSS license information

To fulfill FOSS license obligations, certain information, documentation and other material must be delivered together with the software:

- **Information obligations:** delivering license texts, copyright notices, modification notices, warranty disclaimers, acknowledgments, …
- **Disclosure obligations:** delivering or offering the complete corresponding source code and build and installation instructions
- **Licensing obligations:** adapting company documents (*e.g.* EULA or Terms of Use), licensing own development correctly if a derivative work with software under a copyleft license is created

FOSS license information: Use Cases

- Different **Use Cases** → different aspects to be considered
- The **OSADL Open Source License Obligations Checklists** help to determine what is required (*www.osadl.org/OSLOC*).

FOSS license information: Use Cases (1)

- **Unmodified source code**
  - All required information is generally included.
- **Modified source code**
  - Modification notices (e.g. patches)
  - Correct licensing of modifications

FOSS license information: Use Cases (2)

- **Unmodified or modified binaries**
  - Varies greatly for different licenses: **Checklists** can help (e.g. *OSADL Open Source License Obligations Checklists*)
  - License information must be extracted
  - Possible Copyleft effect on modifications or linked works
- **Software as a Service (SaaS)**
  - Not explicitly handled in most licenses
- **Updates**
  - Separate distribution
  - Publicly available downloads are a preferred target for GPL trolls

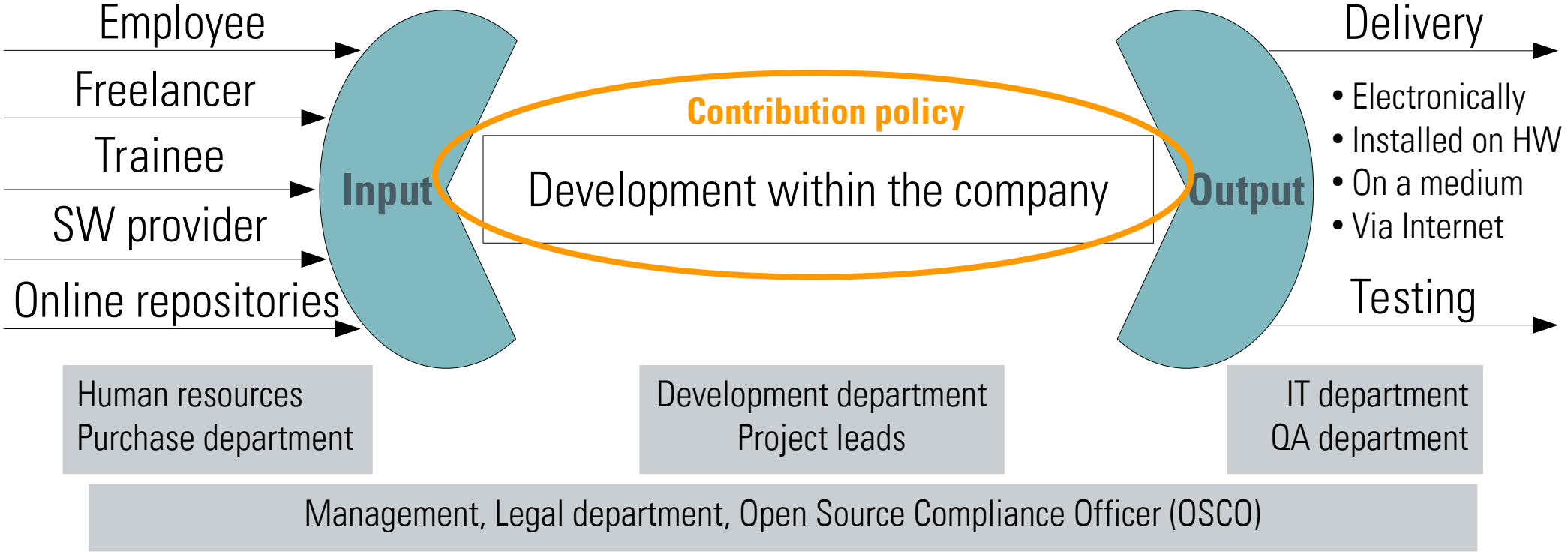
FOSS license information: Use Cases (3)

- **Linuxkernel in an embedded system** (GPL-2.0)
  - Conspicuous notice on use of FOSS and warranty disclaimer
  - Build and installation instructions also for encrypted systems
  - *glibc:* consider obligations of LGPL-2.1 (permit modification and re-engineering of linked proprietary applications)
- **Redistribution of a complete Linux distribution** *(see COOL April)*
  - Copyrights of the software, copyrights of the collective work, trademark rights of the distributor
  - Exhaustion of the distribution right applies for redistribution of unmodified (not installed) versions.

FOSS license information: Delivery

- Creating a **BOM** (Bill of Material) with all FOSS / Software components of a product and their licenses
- **Quality management** (before distribution starts):
  - For every FOSS component listed in the BOM the license information is checked for completeness according to the applicable checklist.
  - **Correcting**, if necessary
- **Releasing** the product for distribution together with FOSS license information

Software flow: Contribution policy



Contribution to FOSS projects (1)

- When a company uses FOSS, they will sooner or later also contribute to FOSS projects.
- **§ 69b UrhG** (German Copyright Act): The employer holds the exclusive rights of use of software that is created by employees in the course of their employment.
- Employees need a **permission**, to license software created in the course of their employment as FOSS.
- A FOSS policy should give guidelines to evaluate a possible contribution

Contribution to FOSS projects (2)

- **Approval of contributor:** training and experience in programming, community etiquette, FOSS licensing, separation of private and company development
- **Approval of FOSS project:** license (copyleft, patents), software quality, reputation, Contributor License Agreements
- **Approval of contribution:** may the contained IP be published, code quality, conflicting agreements (*e.g.* NDA), third-party content, safety and security vulnerabilities

→ **Annex: Contribution permission**

Additional topics (1)

- Communication of the FOSS Policy
  - on the Intranet at *https://intranet.company.tld/FOSS-Policy.pdf*
  - additional provisions in employment contracts:

> […] The employee is obliged to take note of and follow the employer's FOSS Policy immediately after taking up his or her duties. [...]

- Audits and certification
  - OpenChain conformance
  - OSADL License Compliance Audit (LCA)

Additional topics (2)

- Patent considerations:
  - all FOSS licenses require licensing implemented patents
  - Open Invention Network (OIN) and License on Transfer (LOT) Network

- Own FOSS projects
  → Supplement: Selecting a FOSS license

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

II. Open Source Compliance Officer (OSCO)

The Open Source Compliance Officer (OSCO) represents the main contact person of our company in the context of using, copying and distributing FOSS of any kind. He or she coordinates all related activities and maintains a dedicated communication with representatives of the other roles listed below. The OSCO reports to the M and prepares decisions of the M with regard to the following issues:

- (Unclear) interpretation of FOSS licenses that could result in license violations are therefore relevant for the risk management of the company.
- Modification of this FOSS policy.

> The assignment of the OSCO can be documented here or for example on a company's intranet or wiki pages. This decision might depend on how often the assignment changes.

Option 1: Assignment of the OSCO for our company:
Assigned by: *Name*
OSCO name: *Name*
Department: *Department*
Phone number: *Phone number*
Email address: *Email address*
Beginning of the assignment: *Date*
End of the assignment: *Date*
Deputy in case of absence: *Name and Email*
Average week hours to dedicate to the OSCO role: *Hours*

Option 2: The current OSCO for our company is assigned at:
https://wiki.company.tld

VII Use Case 7: Distribution of a Linux kernel in an embedded system

This use cases describes the typical situation that we distribute embedded devices with a Linux kernel under GPL-2.0 and the GNU C Library under LGPL-2.1.

1. Provide the following text as part of the FOSS License Information:

> This product contains third party Open Source Software and Free Software distributed under a number of different licenses (hereinafter referred to as „FOSS"). The respective licenses are listed here, and you can obtain comprehensive rights directly from the right holders to the extent specified therein. The FOSS licenses prevail over all other license conditions and contractual agreements with *company name* with regard to the corresponding FOSS components contained in the product.

2. Fulfill license obligations as given by the → Annex 1: "OSADL Open Source License Obligations Checklists" for the GPL-2.0 (role: PL). In particular the following aspects must be considered:

   - Provide a warranty disclaimer in a conspicuous way by accompanying the product with a note, a section in the manual or a pop-up window on the GUI containing the required information:

> At the request of the copyright holders we point out the following: "This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details."

   - Extract and provide license texts of all licenses and copyright notices contained in the Linux kernel (→ Supplement 2: "How to scan") and deliver them with the product on a data carrier or on the embedded device itself. Notify the recipient of the embedded device where this information can be found.

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*

Disclaimer

Implementing a FOSS policy in a company requires

- **legal expertise**
- (professional and legal) **decision competence** in the name of the company

The template does not replace these qualifications.