Defining a corporate policy
Outbound Open Source @ ZEISS Group

Target group: OSPO OnRamp / OSPO Alliance
Aim: Share best practices in creating a policy that empowers your developers to contribute to Open Source projects

Holger Streidl
Open Source Program Office, ZEISS Digital Partners, Carl Zeiss AG

16 January 2026

Agenda & Introduction

Defining the corporate policy for publicly sharing code

Agenda

1. ZEISS Group & OSPO Overview
2. Open Source Outbound Policy
   - General aspects
   - Risk-based approach
   - Process & Practicalities
3. Discussion and Feedback
   - Overlap with CRA

What is in for you?

- Get to know ZEISS
- Blueprint to define your own outbound policy
- First-hand learnings & experiences

Holger Streidl

- Background in Health IT / Computer Science
  - Not a lawyer, no legal advice
- Long time advocate for Free and Open Source Software (once created Medfloss.org)
- Joined ZEISS in 2019 to build and evolve its Open Source Program
- Roles:
  - Corporate Open Source Officer
  - *New:* (Junior) Departmental Patent Coordinator

Official Journal of the European Union — EN, L series

2024/2847 — 20.11.2024

REGULATION (EU) 2024/2847 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 23 October 2024

on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Manufacturers shall, […] report the vulnerability to the person or entity manufacturing or maintaining the component […]. Where manufacturers have developed a software or hardware modification to address the vulnerability in that component, they shall share the relevant code or documentation with the person or entity manufacturing or maintaining the component, […].

adequate cybersecurity properties or using them in a secure manner.

(2) This Regulation aims to set the boundary conditions for the development of secure products with digital elements by ensuring that hardware and software products are placed on the market with fewer vulnerabilities and that manufacturers take security seriously throughout a product's lifecycle. It also aims to create conditions allowing users to take cybersecurity into account when selecting and using products with digital elements, for example by improving transparency with regard to the support period for products with digital elements made available on the market.

CRA – Article 13 (6)

ZEISS Group

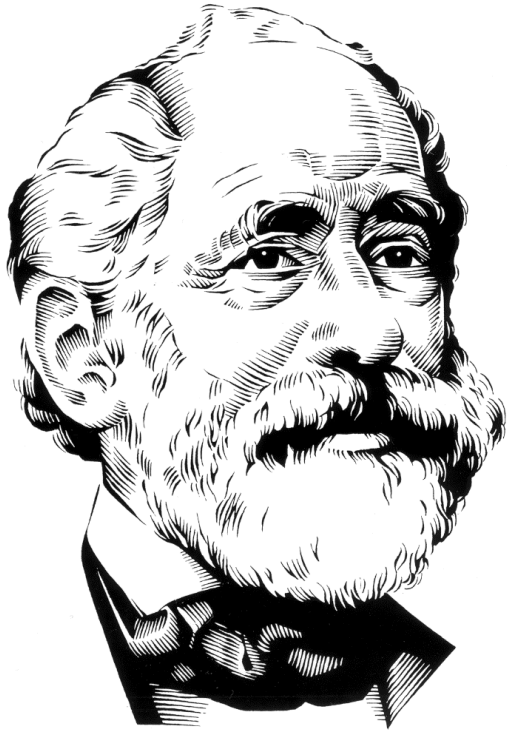
As the pioneer of science in optics, we continue to challenge the limits of human imagination.

Enabling customers
Founder and partner

A strong foundation for a strong future

Carl Zeiss founded a workshop for precision mechanics and optical instruments in Jena in 1846. Ernst Abbe – a young scientist – later joined the company and became a partner in 1876.

Optical technologies pave the way for many innovations. Carl Zeiss and Ernst Abbe recognized this early on, and this led to the creation of innovative new products and technologies that enabled the company to meet its customers' needs.



Carl Zeiss
Founder

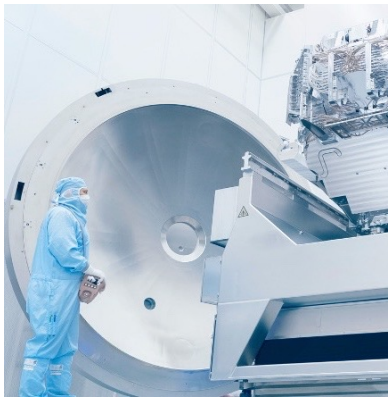
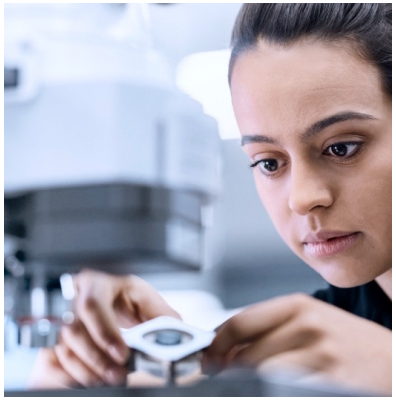
Ernst Abbe
Partner

Enabling customers
Microscopy solutions from ZEISS

In 1857, Carl Zeiss developed his first microscope with an assembled optical system. In the following years, microscopy solutions from ZEISS became increasingly powerful and enabled significant scientific progress.

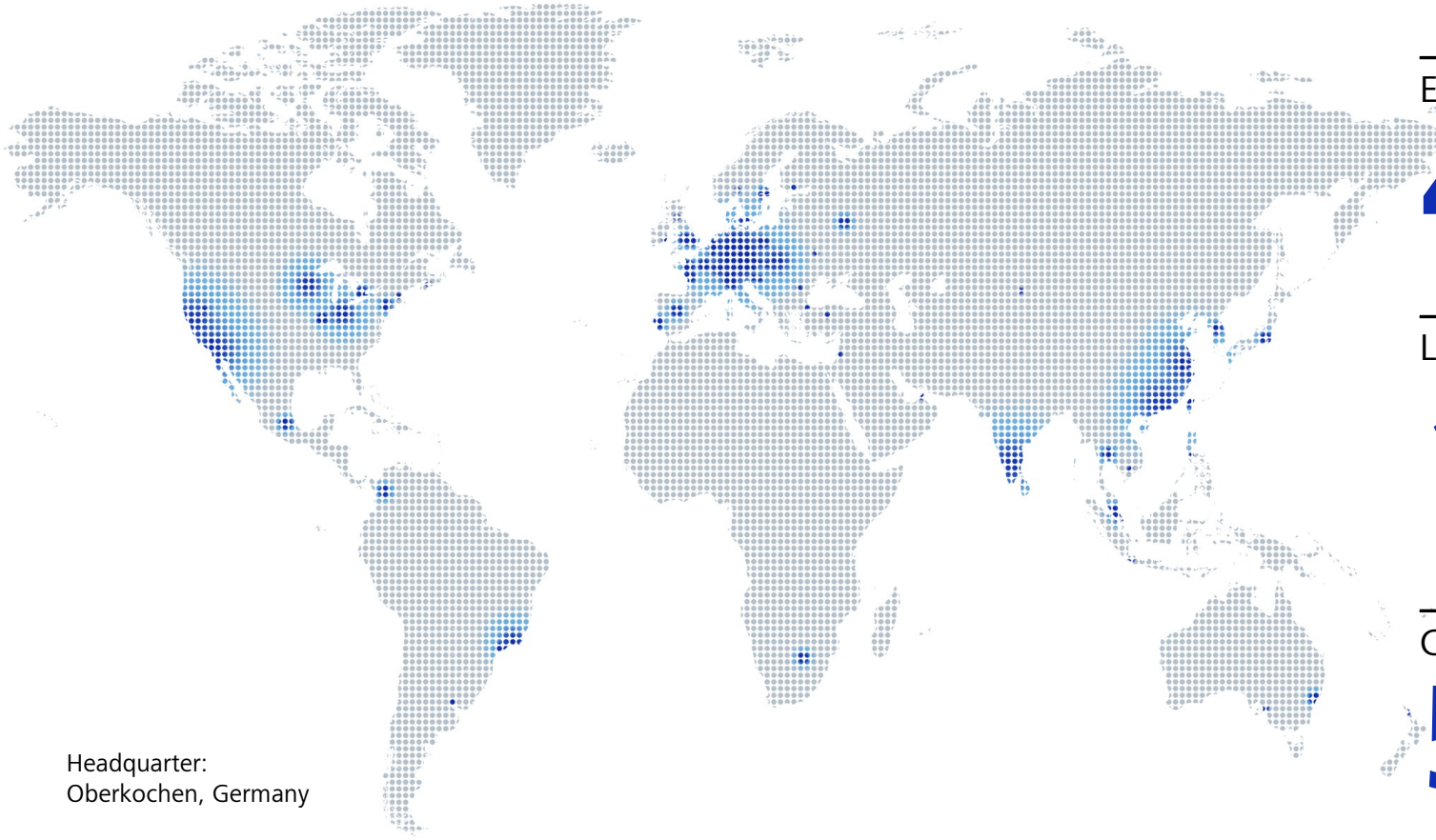
Microscopy solutions from ZEISS helped Robert Koch identify tuberculosis bacteria. And this was a key to fighting it.

Shaping the future
The ZEISS Segments and Strategic Business Units

Semiconductor Manufacturing Technology	Industrial Quality & Research	Medical Technology	Consumer Markets	
				
Strategic Business Units ▪ Semiconductor Manufacturing Optics ▪ Semiconductor Mask Solutions ▪ Process Control Solutions	▪ Industrial Quality Solutions ▪ Research Microscopy Solutions	▪ Ophthalmology ▪ Microsurgery	▪ Vision Care ▪ Extended Reality *Started in FY 2025/26*	▪ Photonics & Optics *Specialized businesses beyond ZEISS Segments*

ZEISS worldwide

As of FY 2024/25



Headquarter:
Oberkochen, Germany

Employees (Headcount)

46,622

Locations worldwide (rounded)

100

Countries (rounded)

50

16 January 2026

Investment in research & development

Facts

Innovation shapes the future: research and development teams at ZEISS are working hard to constantly expand our role as a technology leader and market shaper. ZEISS has been making sustainable investments in R&D in order to achieve this goal.

New patent applications

730

R&D investments in € million

1,731

Investments by % of revenue

15%

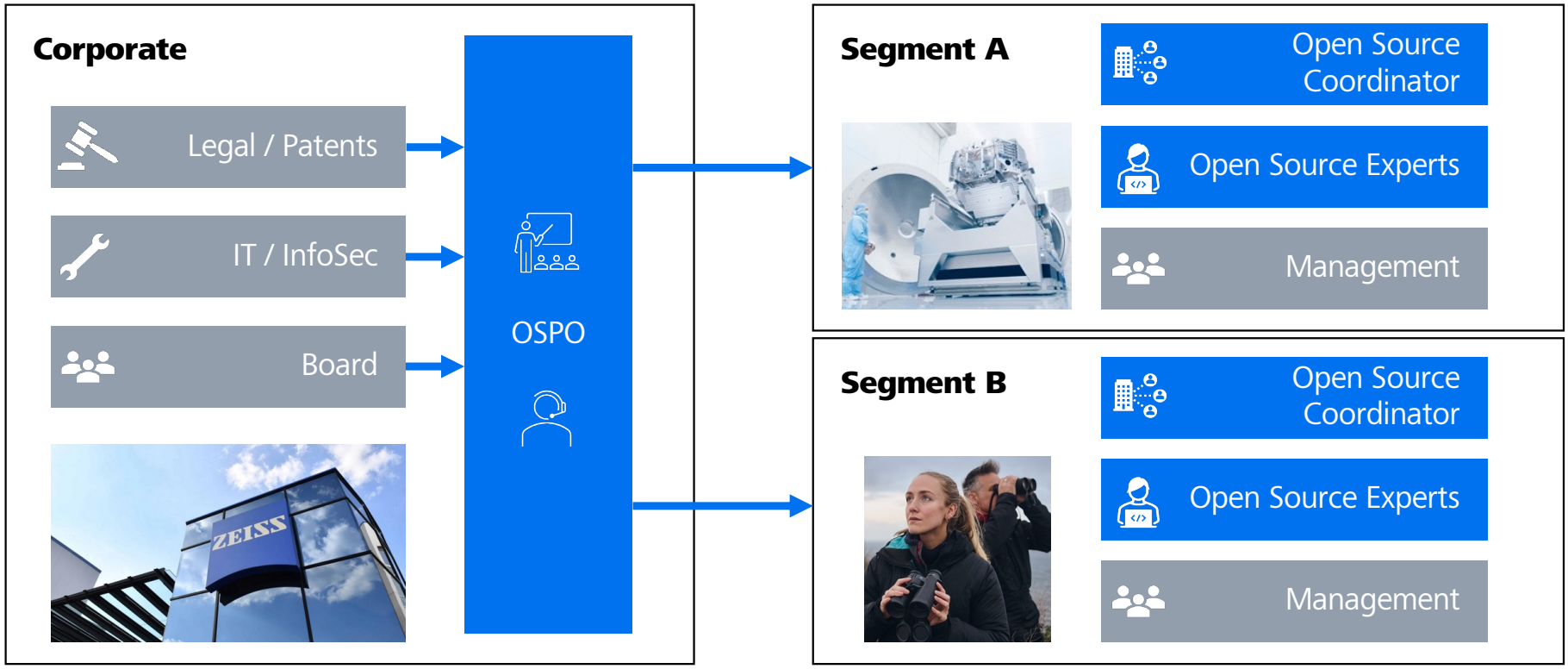
16 January 2026

Open Source Governance

Controlling Risks, Reaping Benefits

Open Source Governance within ZEISS Group

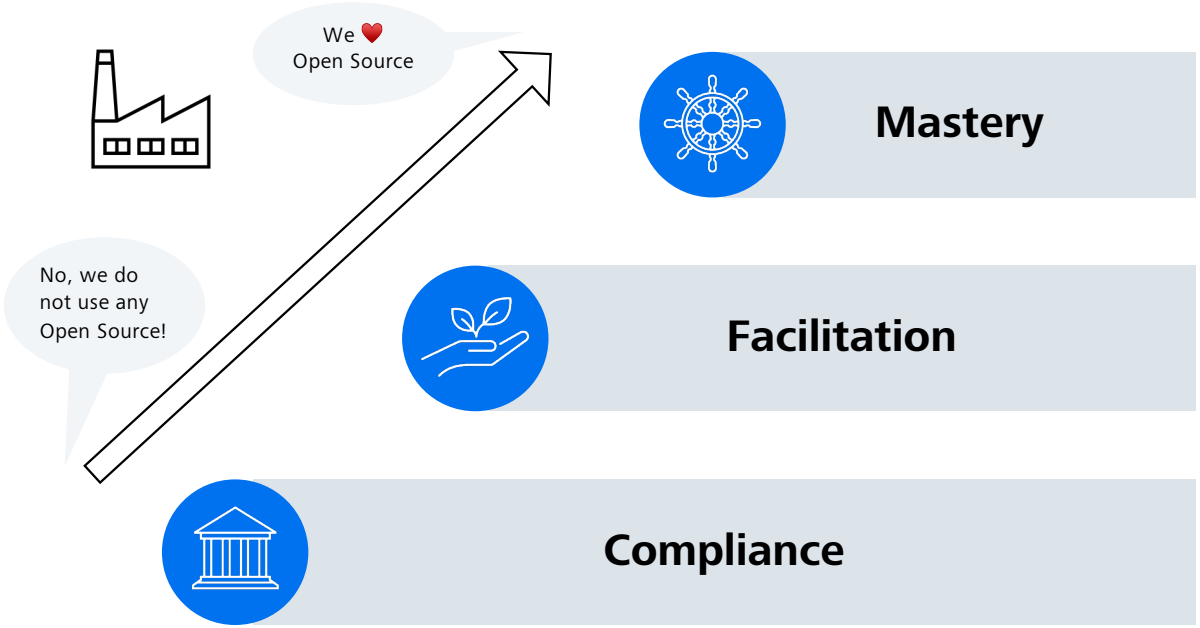
OSPO as central competence center, local self-dependent fulfillment



Stepwise evolution of Open Source adoption

Turning uncontrolled risks into strategic opportunities

Phases



Actions

Open Source becomes a strategic asset.
Company actively joins community.
Drive and release Open Source projects.

Added value is acknowledged.
Company starts interacting with community.
Contribute to Open Source projects.

Awareness that Open Source is omnipresent.
Company must control its risks.
License fulfillment and vulnerability mitigation.

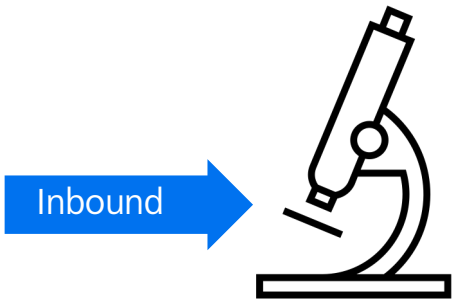
Context

Setting the scene …

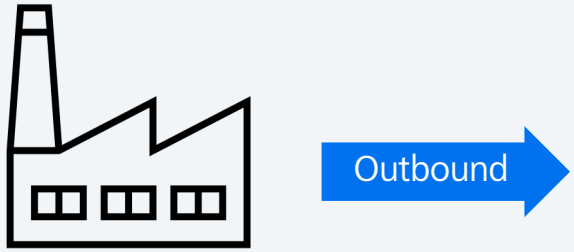
Inbound vs. Outbound

Integrating vs. contributing/releasing Free and Open Source Software (FOSS)

Building products with FOSS components



Contributing to and releasing FOSS projects



Shopping List

Empower employees to reap the power of collaborative SW engineering

What we want

- Enable contributions and active engagement
- Clear and easy to understand guidance, with as few bureaucracy as required

Underlying assumptions

- Process is typically initiated by developer
- Developers can act self-dependent
- Fixes and minor improvements are dominant
- Business units have established state-of-the-art software development (processes)

What could possibly go wrong

- IP loss or conflict
- Security incident
- Lack of resources
- Reputational damage

General Criteria

Drafting a corporate policy for contributing to Open Source projects

Why should we allow our developers to contribute?

We pay them to work on our products!

How much of your product's code base is Open Source?

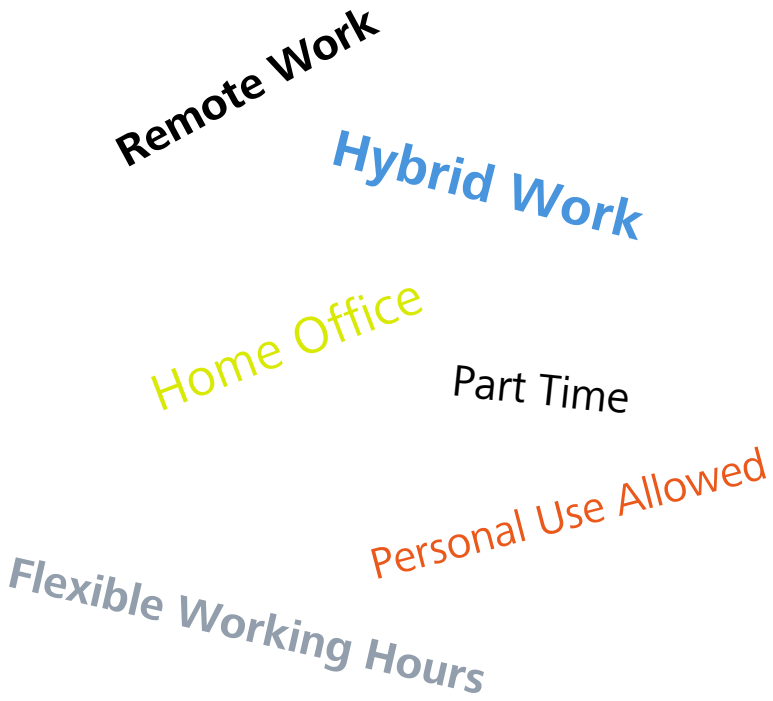
Well, … For further motivation:

- Look into your software composition analysis (SCA) results
- Refer to the annual reports of SCA vendors (Security & Risk Analysis Report)
- Refer to LF's "Open Source as Europe's Strategic Advantage" Research Report 2025
- Refer to Bitkom's "Open Source Monitor 2025"

Who is making sure that those work for our use case? Secure, stable, …

Why should we keep fixes local? Additional effort to merge with upstream changes …

When shall the policy apply?
Defining „Work Context“



Scope of Policy

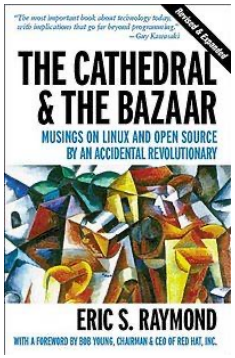
- Working hours / “on-duty”
- Company-specific knowledge
- Company identity

When does it make sense to consider contributing/publishing?

Good reasons to justify involved effort and risk

"Everything should be open …"

"The community will fix it …"



„Every good work of software starts by scratching a developer's personal itch.", **Eric S. Raymond** in *the Cathedral and the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary (1999)*

Basic Criteria

- Beneficial for product or business in general
- In-line to overall goals of ZEISS Group and ZEISS Foundation
- Relevant and potentially beneficial for the community

What can and cannot be published (contributed)?

Protect differentiating intellectual property and knowledge

"The Crown Jewels“, source: https://commons.wikimedia.org/wiki/File:Crown_Jewels_of_the_United_Kingdom_1952-12-13.jpg

Probably not well suited to share …

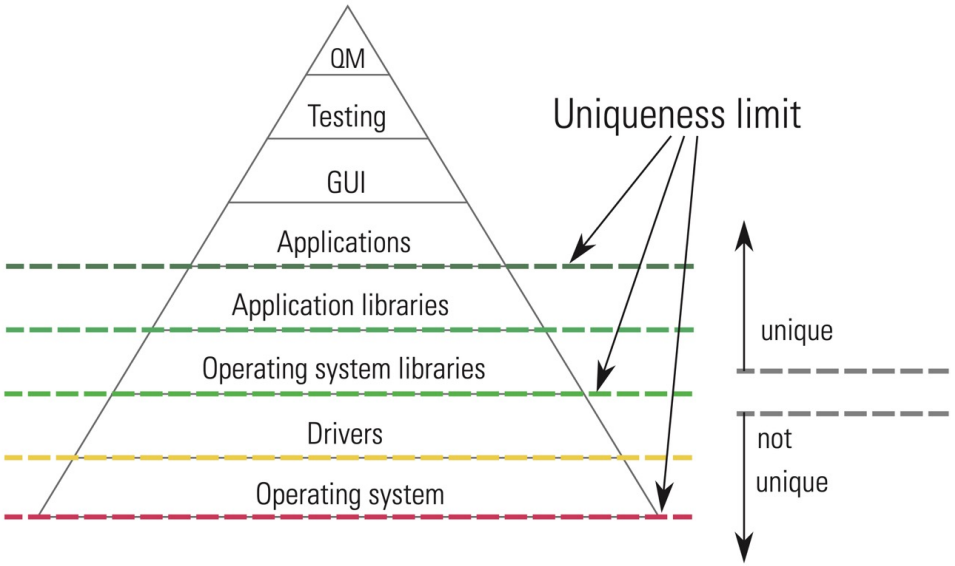
- Specific to ZEISS, not known to competitors, would reduce our competitiveness if it was
- Strategic character, enabler or core to our business
- Novel compared to state-of-the-art
- Significant investment for its creation (R&D)

Out of scope …

- Inventions (patent application), trade secrets, or just confidential

What code is best suited for an Open Source Release?

Share and collaborate on non-competing assets



“Uniqueness pyramid”

Source: Whitepaper ¨Free and Open Source Software (FOSS), OSADL
Link: https://www.osadl.org/Paperless-OSADL-Brochures.online-info.0.html

Typically well suited for public release

- Non-specific to our company, mostly exchangeable
- Supporting/foundational technology (DE: “Basistechnologie”)
- Operative character, supportive to our products and services
- Would it work even when our strongest competitor(s) joins?

Risk-based approach

Controlling risk based on the amount of code to be shared

Bug fix / minor improvement to existing functionality

No risk – self-responsible contribution

Source Code

Bug Fix / Improvement	
No approval required.	Only existing code is modified. No risk that confidential code is shared. Simplicity shall facilitate contributions.

New functionality for already public code

Minor risk requiring only limited approval

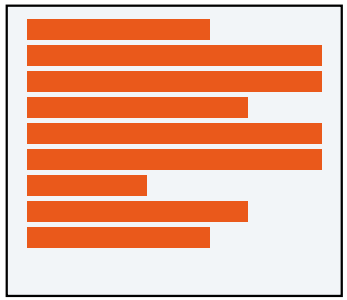
Source Code

New Feature	
Project-level approval required.	Portions of new code are shared externally. Minor risk that confidential functionality is accidentally released. Limited review shall assure conformity.

Entire software (code base) to be published

More risk requiring detailed review and approval

Source Code



New Project	
Department-level approval required.	Entire project is shared externally. Risk that competitive advantage might be lost. Resources need to be assigned to work with community. Full review essential.

Process Aspects

Controlling Risks, Reaping Benefits

Important Intellectual Property Aspects

Re-use and protection of work and inventions

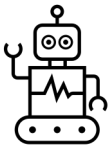
When providing contributions (outgoing)

- Can we still use code that we shared in own proprietary/closed applications? (non-exclusive license)
- Any indemnity or warranty claims that we cannot fulfill? (disclaimer)
- Can we still apply for a patent and practice/enforce our patent? (state-of-art, implicit/explicit patent grant)

When receiving contributions (incoming)

- Are contributors original authors and entitled to grant usage license / transfer copyright?
- Any patents involved that might introduce restrictions?
- Can contributions be used in own proprietary / closed applications and products? (sub-license)

- Contributor License Agreement (CLA)
- Developer Certificate of Origin (DCO)



- LLM-based Coding Assistants

Example: Approver for a full-grown project

Responsibilities to support release process

- **Head of Department**
  - Overall assessment of suitability. No plans for commercialization?
  - Resource assignment and planning
- **Patent Coordinator**
  - FTO, patent infringement
  - Patent application
- **Legal Advisor**
  - Licensing constraints
  - Copyright assignment / re-use
- **Corporate Open Source Officer**
  - Best practices
  - „Partner in Crime“
- **Project Maintainer**
  - Nomination & awareness
  - Proxies

Challenges

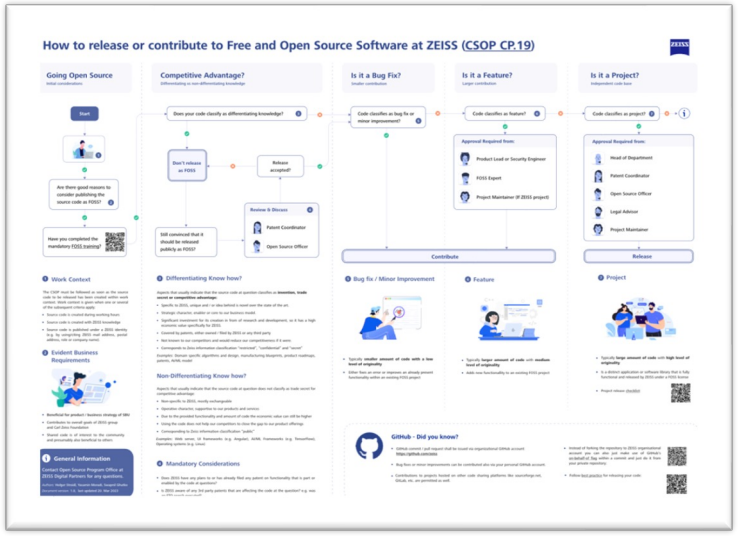
- Are roles/responsibilities available in every team and named like that?
- Who is my responsible person? (contact list)
- Synchronous vs. asynchronous review and approval
- Persistent evidence

Practicalities

Getting the details right

Facilitating proper implementation
Beyond a pure formal policy

- Abstraction layers
  - **What?** Formal guideline/policy
  - **How?** Wiki, training, templates, case-specific support
- **Mandated training**
- Improved **accessibility** of policy: Illustrated process



Detailed **checklist** with further explanation of important aspects to consider

- Essential files (LICENSE, README, CONTRIBUTING, …)
- Licensing markup according to https://reuse.software/
- Documentation and code comments
- No encryption keys, passwords, internal URLs
- No confidential data (personal data, product data, …)

Working with code hosting platforms
Committing and monitoring

- GitHub is not and **never** was the one and only **source code hub** (e.g. Codeberg, self-hosting, …)
- Not only a strategic questions: policy **must be platform agnostic**
- How to sign/confirm licensing terms
  - Sign off (--signoff, -s) for license, CLA, …
  - SAP's CLA Assistant (https://cla-assistant.io/)
  - LF's EasyCLA (https://easycla.lfx.linuxfoundation.org/)
- For GitHub
  - Personal or company handle?
  - On behalf (on-behalf-of)
- User administration via IT department (incl. offboarding)

Monitoring and metrics

- Regular monitor own hosting platform for **non-compliant** or **non-relevant** repositories
- Assess and present community engagement
  - OSS Contributor Index (https://opensourceindex.io/)
  - GH Archive (https://www.gharchive.org/)

Off-topic as not Open Source specific

Prevent duplication and instead reference to other policies

Minimize overlap with other **corporate policies**

- Quality
- Security (+ CRA)
- Privacy
- Netiquette

Discussion

CRA & Improvement Opportunities

EU Cyber Resilience Act (CRA) & Outbound Policy

Important element within the company-wide implementation

Will our FOSS Outbound Policy be the central means to implement the CRA at ZEISS?

No, but …

Open question

- Are we "**manufacturer**" (!) or "**steward**" (?) according to CRA of our own Open Source projects?

Important adjustments

- **Priority-track** for **vulnerability fix** contributions
- Document and archive **evidence**
- Mandate **SBOM** for our FOSS projects
- … for our Inbound Policy:
  - Mandate upstream **vulnerability reporting**
  - Mandate upstream **security fix sharing**

Increased criticality of "maintainer" role

- Handle external reports and bug fixes
- Regular screening and analysis

Challenges and improvement opportunities
Topics and backlog

- Hardware vs. software innovation
- Management awareness and support
- Heterogenous infrastructure (development platforms, document mgmt. systems)
- Integrated/seamless end-to-end process, incl. CLA/DCO management
- Incentivize active engagement
- Dedicated “community manager”
- Connect to Inner Source as “graduation”

... what else are you missing or would you improve?

Thank you for your interest and attention!

Question & Answers

Looking forward to your questions and feedback!

Holger Streidl

Open Source Program Office
ZEISS Digital Partners, ZEISS Group

Mail: <first>.<last>@zeiss.com
LinkedIn: https://www.linkedin.com/in/holgerstreidl/

We are **hiring** at OSPO@ZEISS, check https://zeiss.ly/ospo-job

… not yet live, will be posted soon.

Seeing beyond