Requirements and State of the Art of Open Source License Compliance Tooling

Mirko Boehm
Open Compliance Summit 2017
Yokohama, Japan
@mirkoboehm

About Me: Free and Open Source Software Contributor

Founder and CEO, Endocode.

Director, Linux System Definition, Open Invention Network.

KDE contributor since 1997, former board member.

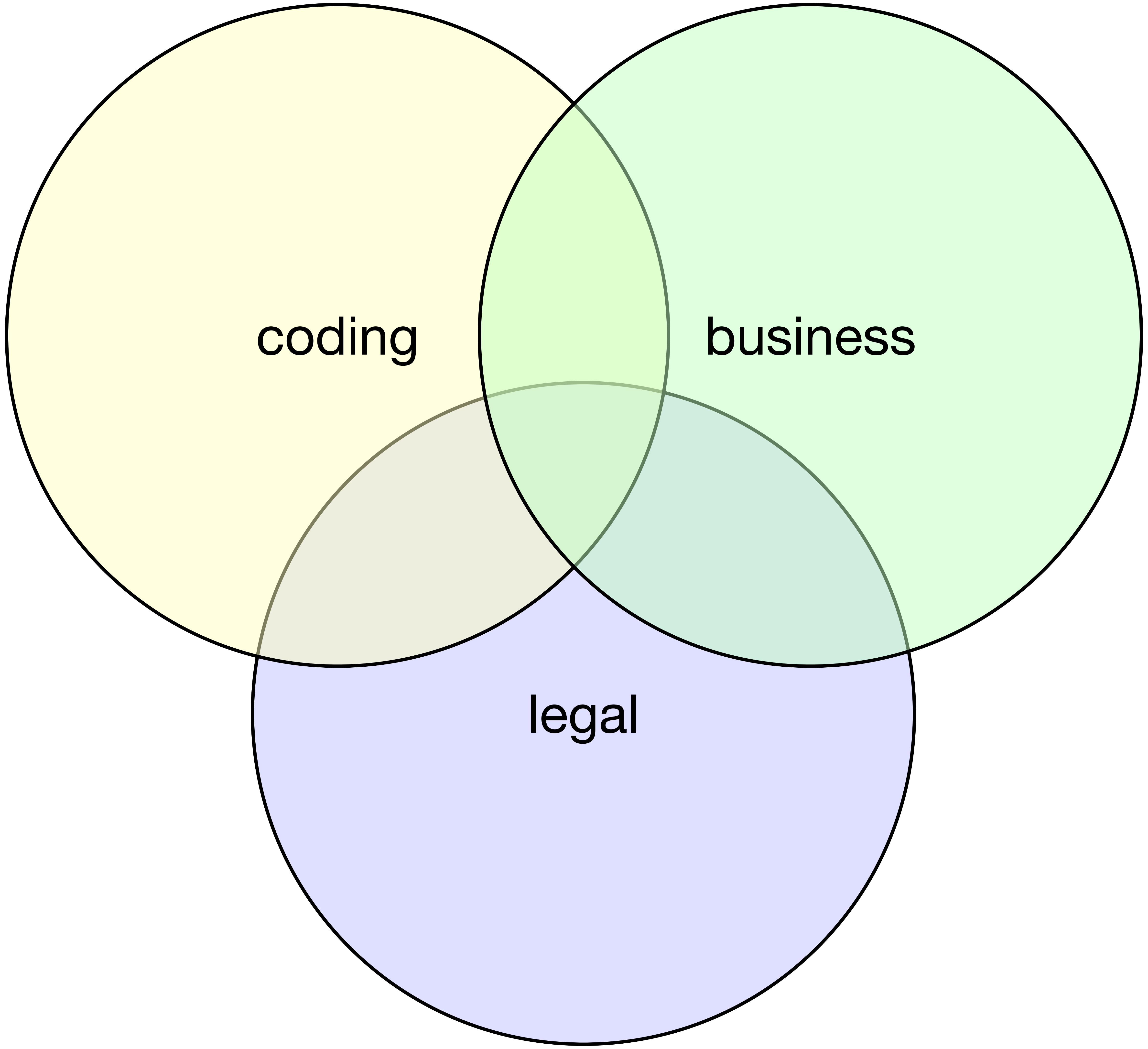
Visiting lecturer and researcher at the Technical University of Berlin.

Fellowship representative in the FSFE general assembly, Legal Network.

Openforum Academy fellow.

Requirements: Legal - Business - Software Engineering

The FLOSS Compliance Skill Conundrum



Requirements from a **legal** perspective

- peace of mind: be sure all primary and secondary license obligation are met, for all products, all the time
- well-defined review processes to make compliance decisions for software
- create and archive accompanying audit documents with every software release

Requirements from a **business** perspective

- quality (management problem): compliance is an obligation, a business process is needed that solves the problem at the expected quality level

- cost: cost should be negligible compared to the product development cost

- organisation: compliance needs to smoothly integrate into other business processes (product management, logistics, supply chain, long-term reliability)

Requirements from a **engineering** perspective

- Pace/velocity: In most environments, software is now released early and often. There is no "stable release" that legal can review.

- Open collaboration: Software is released in public repositories, every commit is a release.

- Workflow: CI is the central hub of software engineering

- Technical requirements: Diverse environments. Multiple relevant build systems. languages, runtimes and frameworks change. Tooling needs to be agnostic

> “**Hygiene factors** … do not give positive satisfaction or lead to higher motivation, though **dissatisfaction** results from their absence.”

–Two-factor theory (Wikipedia)

FLOSS Compliance as a **hygiene factor**:

Coders believe license obligations simply should be kept. This is **the spirit of Open Source**, and how hard can it really be?

There is a need to **pragmatically automate the compliance workflow** where it can be automated.

Individual tools exist, but **no industry standard workflow or toolchain** have emerged.

FLOSS Compliance Tooling as a **Governance** Problem:

- Avoid appropriation.
- Solve fragmentation.
- Don’t be opinionated.

Introduction to Quartermaster

QMSTR creates an **integrated Open Source toolchain** that implements industry best practises of license compliance management.

Mission

Paradigms

- Open Source Compliance Tooling itself needs to be Open Source.
- Implement what is missing (workflow toolchain), reuse what exists.
- Most code gets maintained, not developed from scratch.
- Collaborate with legal and business stakeholders.

Feature Overview

Integration into **DevOps** **CI/CD** cycles.

Feature Overview

Native support for all major **software build** systems.

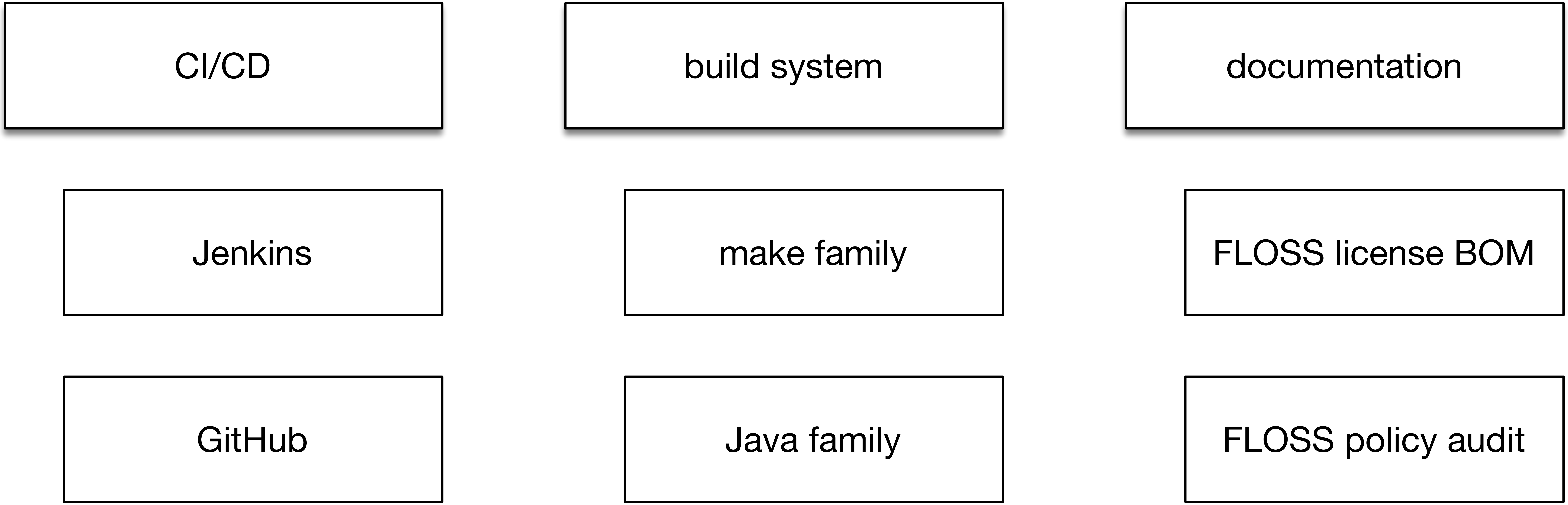
Feature Overview

Command line toolchain.

Feature Overview

Customisable **integration** into **DevOps CI/CD workflow**, knowledge bases and documentation generators.

Year 1 Project Vision



CI/CD

- Jenkins
- GitHub

build system

- make family
- Java family

documentation

- FLOSS license BOM
- FLOSS policy audit

APIs, not file formats

- “Integrations" communicate with the QMSTR master through a REST API.
- Plugins not compatible with QMSTR strict copyleft license can be implemented as separate processes communicating through the API.
- This allows to integrate existing tooling (license scanners, …) into the QMSTR workflow.

Adding the missing bit to the Open Compliance Program

SPDX

QUARTERMASTER

OPENCHAIN

Roadmap

- Q4/2017: Minimum viable prototype.
- Q1/2018: First beta release. Potentially formation of QMSTR as a Linux Foundation project.
- 06/2018: First production release.
- After that: A major release every three months.

How to get involved

Project Setup

- Quartermaster is currently run by Endocode.
- Quartermaster plans to move to Linux Foundation - this needs your support!
- Current velocity: 2 week sprints, quarterly milestones.

>_ ENDOCODE

Join the conversation!

- Visit https://join.slack.com/t/qmstr/signup to join the Slack workspace.
- Email qmstr-announce+subscribe@endocode.com (or mirko@endocode.com) to subscribe to the Quartermaster Announcements mailing list.
- Watch qmstr.org for updates.

How to support the Quartermaster project!

- Indicate interest and/or intention to join the project to LF Open Compliance program.
- Contribute financial support through a grant to Endocode.
  - or…
- Contribute code by dedicating engineering capacity.

Summary

- QMSTR aims at building the **industry standard** for Open Source compliance tooling.

- QMSTR will itself be Open Source.

- QMSTR integrates with existing Linux Foundation **Open Compliance** projects, like OpenChain, SPDX and Fossology.

- Get involved and help **make license compliance the default**!

Quartermaster

Open Source Compliance Tooling

Mirko Boehm
Open Compliance Summit 2017
Yokohama, Japan
@mirkoboehm