Open Source
Tooling Group

The OpenChain Reference Tooling Work Group

The OpenChain reference tooling work group 2021

Situation today

The use of OSS in products and services is increasing exponentially

The OSS compliance process needs to be as automated as possible and fully integrated in the CI/CD pipelines

An integrated OSS compliance toolchain needs to be modular, flexible and adaptable

Objective and purpose

We are building an open source compliance toolchain ecosystem with open source tools as an open source project.
To accomplish this we:

- Use existing independent tooling projects
- Provide reference workflows to allow their adoption
- Provide the concepts and glue to ensure easy interoperability and integration in existing environments
- Provide reference turnkey toolchains that can be used without fees by anybody

The Approach

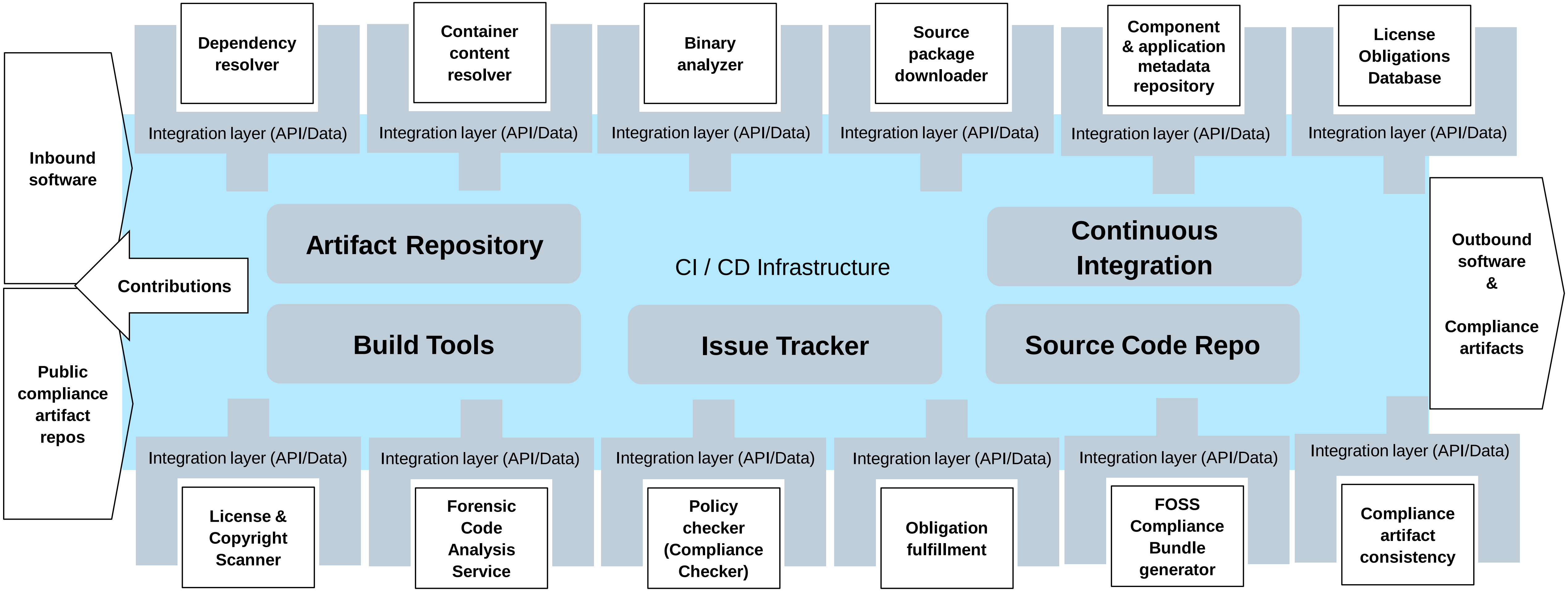
Available epics – how users interact with the toolchain and what information they are requiring for accomplishing their tasks

The functional building blocks and capabilities are described

Example workflow and the flow of information is available

First version of a data model is available

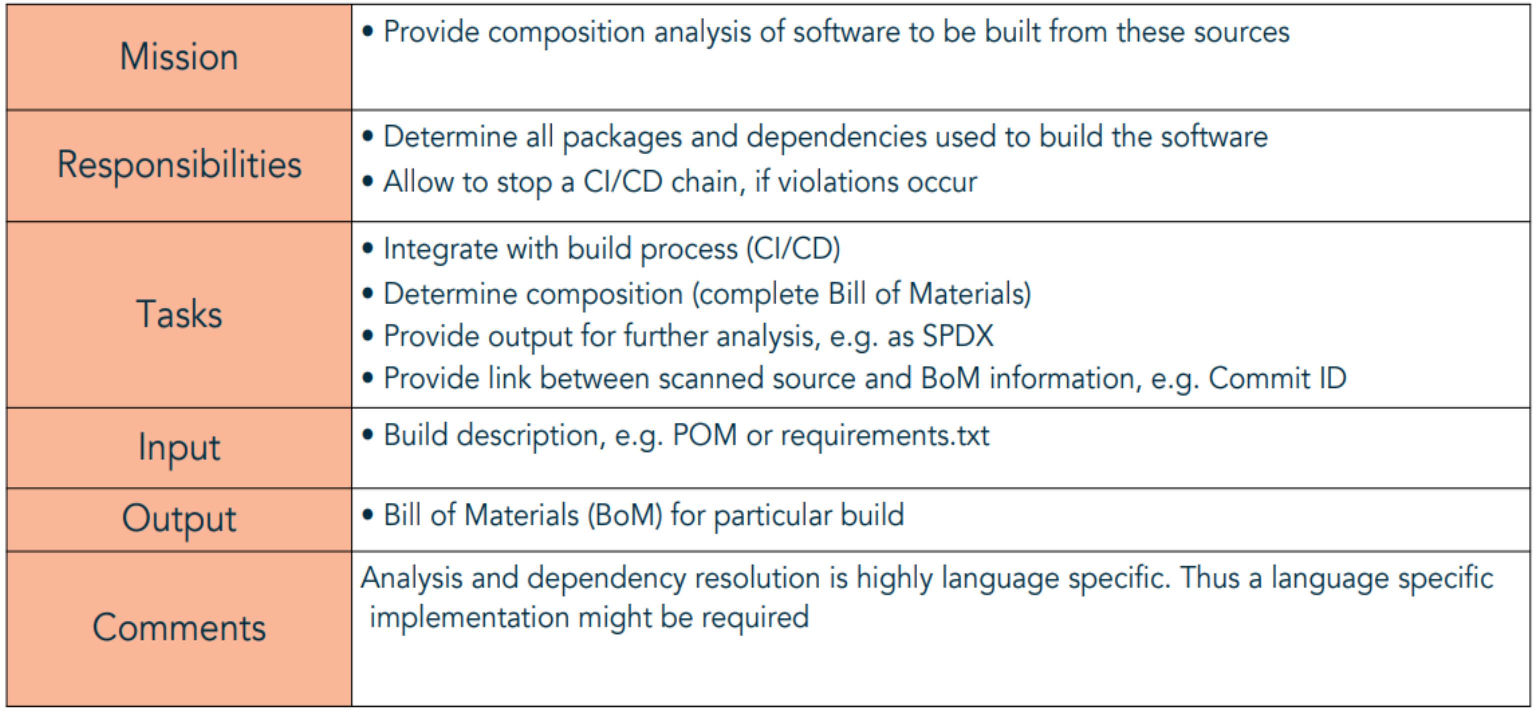
Big Picture – Integrated Compliance Toolchain


Dependency resolver
Container content resolver
Binary analyzer
Source package downloader
Component & application metadata repository
License Obligations Database
Integration layer (API/Data)
Integration layer (API/Data)
Integration layer (API/Data)
Integration layer (API/Data)
Integration layer (API/Data)
Integration layer (API/Data)
Inbound software
Artifact Repository
CI / CD Infrastructure
Continuous Integration
Outbound software & Compliance artifacts
Contributions
Build Tools
Issue Tracker
Source Code Repo
Public compliance artifact repos
Integration layer (API/Data)
Integration layer (API/Data)
Integration layer (API/Data)
Integration layer (API/Data)
Integration layer (API/Data)
Integration layer (API/Data)
License & Copyright Scanner
Forensic Code Analysis Service
Policy checker (Compliance Checker)
Obligation fulfillment
FOSS Compliance Bundle generator
Compliance artifact consistency

Toolchain elements and capabilities

Dependency Resolver

A tool that determines the dependencies of software projects. It is technology and package manager specific how dependencies are expressed - thus there need to be dedicated functionality of the different package managers in use. The dependency resolver ensures the all dependencies are resolved recursively. It ensures that the output is a technology and package manager neutral complete list of dependencies.



Mission	• Provide composition analysis of software to be built from these sources
Responsibilities	• Determine all packages and dependencies used to build the software • Allow to stop a CI/CD chain, if violations occur
Tasks	• Integrate with build process (CI/CD) • Determine composition (complete Bill of Materials) • Provide output for further analysis, e.g. as SPDX • Provide link between scanned source and BoM information, e.g. Commit ID
Input	• Build description, e.g. POM or requirements.txt
Output	• Bill of Materials (BoM) for particular build
Comments	Analysis and dependency resolution is highly language specific. Thus a language specific implementation might be required

New and identified Tools

ScanCode.io

https://scancodeio.readthedocs.io/en/latest/

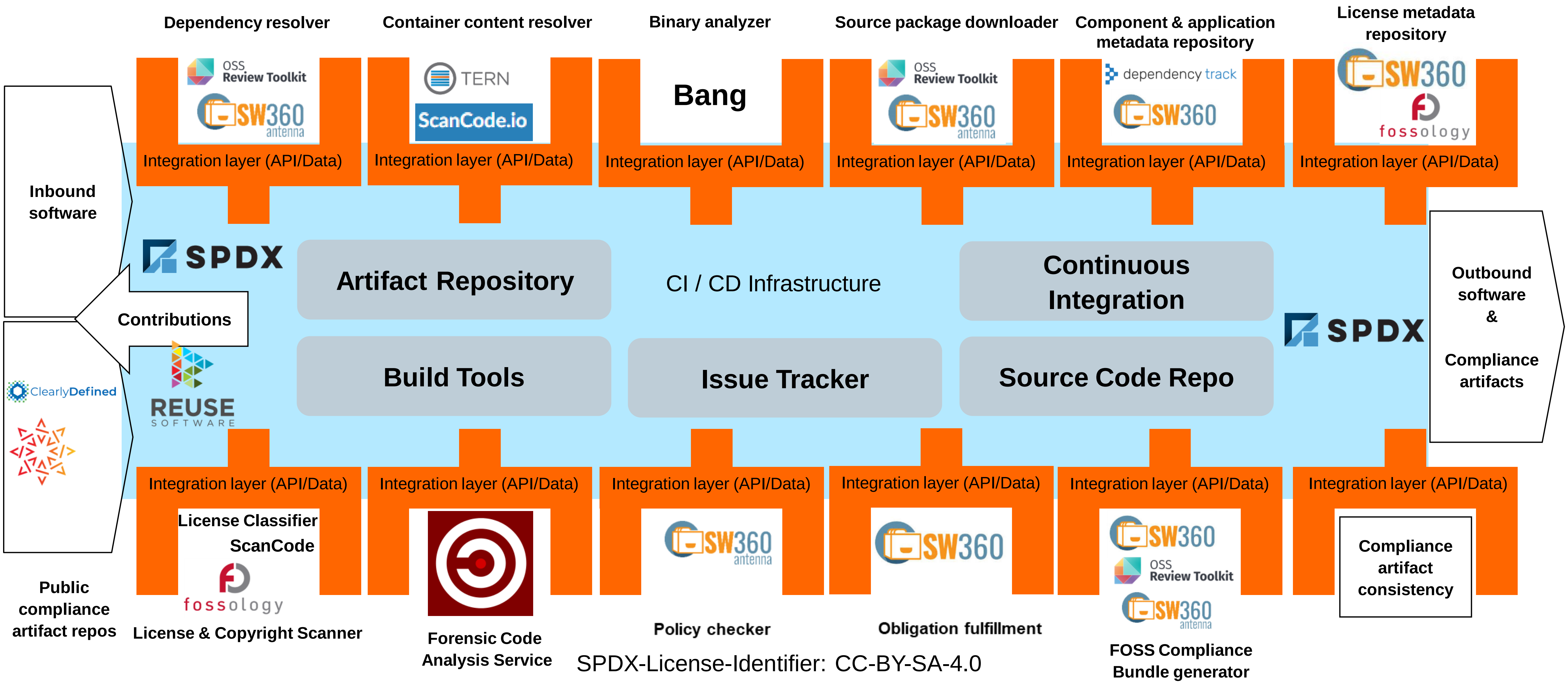
dependency track

https://dependencytrack.org/

https://www.scanoss.com/

https://optum.github.io/barista/

Example Automation Implementation Using Open Source Tools



Dependency resolver

OSS Review Toolkit

SW360 antenna

Integration layer (API/Data)

Container content resolver

TERN

ScanCode.io

Integration layer (API/Data)

Binary analyzer

Bang

Integration layer (API/Data)

Source package downloader

OSS Review Toolkit

SW360 antenna

Integration layer (API/Data)

Component & application metadata repository

dependency track

SW360

Integration layer (API/Data)

License metadata repository

SW360

fossology

Integration layer (API/Data)

Inbound software

SPDX

Contributions

REUSE SOFTWARE

ClearlyDefined

Public compliance artifact repos

Artifact Repository

CI / CD Infrastructure

Continuous Integration

Build Tools

Issue Tracker

Source Code Repo

SPDX

Outbound software & Compliance artifacts

Integration layer (API/Data)

License Classifier

ScanCode

fossology

License & Copyright Scanner

Integration layer (API/Data)

Forensic Code Analysis Service

Integration layer (API/Data)

SW360 antenna

Policy checker

Integration layer (API/Data)

SW360

Obligation fulfillment

Integration layer (API/Data)

SW360

OSS Review Toolkit

SW360 antenna

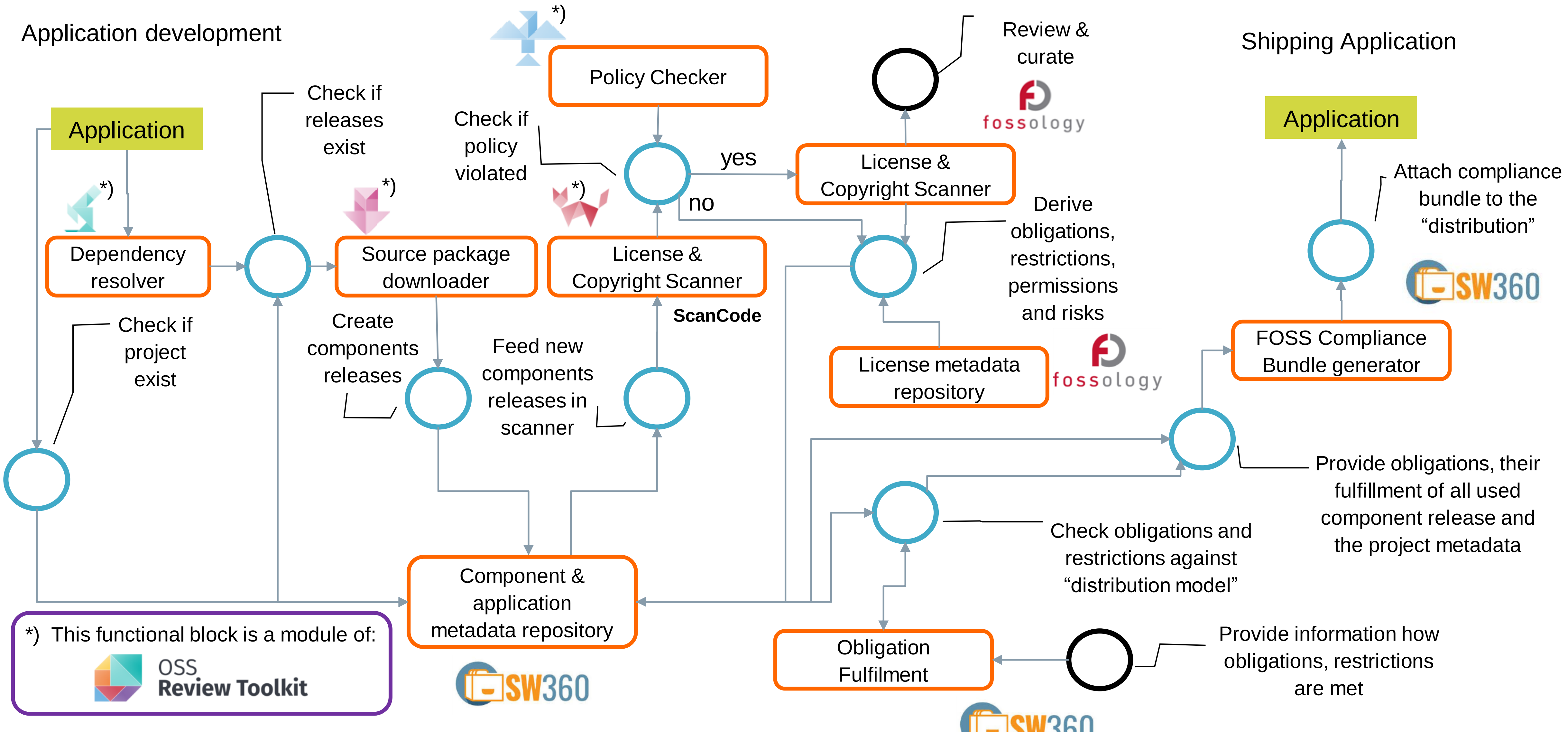
FOSS Compliance Bundle generator

Integration layer (API/Data)

Compliance artifact consistency

Example reference workflow

Open Source Tooling Group



Application development

Application

Dependency resolver

Check if project exist

Check if releases exist

Source package downloader

Create components releases

Check if policy violated

Policy Checker

yes

no

License & Copyright Scanner

ScanCode

Feed new components releases in scanner

Component & application metadata repository

License & Copyright Scanner

Review & curate

fossology

Derive obligations, restrictions, permissions and risks

License metadata repository

fossology

Check obligations and restrictions against "distribution model"

Obligation Fulfilment

Provide information how obligations, restrictions are met

Provide obligations, their fulfillment of all used component release and the project metadata

FOSS Compliance Bundle generator

Attach compliance bundle to the "distribution"

Shipping Application

Application

SW360

*) This functional block is a module of: OSS Review Toolkit

OSS compliance toolchain things to do

Further reference workflows need to be described

Reference set ups need to be done and maintained

- Functional glue code need to be implemented
- Integrations need to be tested and described
- Tutorials need to be provided

The required tools / functionality is available the only thing which is needed is the integration

Pain points

We urgently need developers, who are able to work continuously on integration scenarios and publish the code under an OSS license

We need marketing on OSS solutions and successful integration scenarios

In short words

Open Source
Tooling Group

OSS license compliance for everyone

This is what we do

Your help and expertise is highly welcome

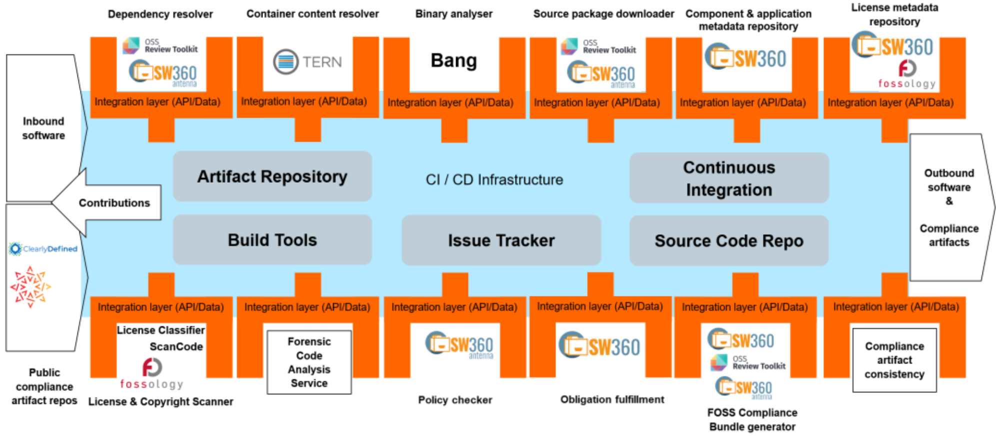
Reference Tooling Work Group

We are building an open source compliance toolchain ecosystem with open source tools as an open source project.
To accomplish this we:

- Use existing independent tooling projects
- Provide reference workflows to allow their adoption
- Provide the concepts and glue to ensure easy interoperability and integration in existing environments
- Provide reference turnkey toolchains that can be used without fees by anybody

World-Wide Collaboration, World-Wide Availability

Example Automation Implementation Using Open Source Tools



Join Us in Creating a New Era for Open Source Compliance

Mailing List: oss-based-compliance-tooling@groups.io

Subscription page: https://groups.io/g/oss-based-compliance-tooling

Online meetings: Bi-weekly - Invitations are sent to the mailing list

Website: https://oss-compliance-tooling.org/

And of course we are on GitHub:

https://github.com/Open-Source-Compliance/Sharing-creates-value

How to get involved

Github:
https://github.com/Open-Source-Compliance/Sharing-creates-value

Slack:
https://join.slack.com/t/ossbasedcompl-bhx9742/shared_invite/enQtODE2MTMxNzUyNDY1LWQyNWVlNzkyMjhhOWUyNDdjNDJlMzk0YzU0NDUwNzQ2YzY0Mzc1N2Y2NjhhZGEyN2JmNDE0ZTg2MTBjYmM3MWI

Mailing List:

Subscription page: https://groups.io/g/oss-based-compliance-tooling

Email address: oss-based-compliance-tooling@groups.io

Thank you