Automating FOSS reviews for a large company with a small team

Photo by Marvin Mayer on Unsplash

About me

thomas.steenbergen@here.com
@tsteenbe
linkedin.com/in/tsteenbe

Head of Open Source

- HERE Open Source Office (OSO) is a team of 7 people
- Supporting 9k+ employees in 56 countries on all things Open Source together with our legal counsels

Active contributor to:

OSS Review Toolkit
http://oss-review-toolkit.org

SPDX

Open Source Tooling Group

OPENCHAIN

ClearlyDefined

TODO
European Chapter

Why: Open Source Compliance Program

OPENCHAIN

- **Know your obligations.** You should have a process for identifying and tracking Open Source components that are present in your software

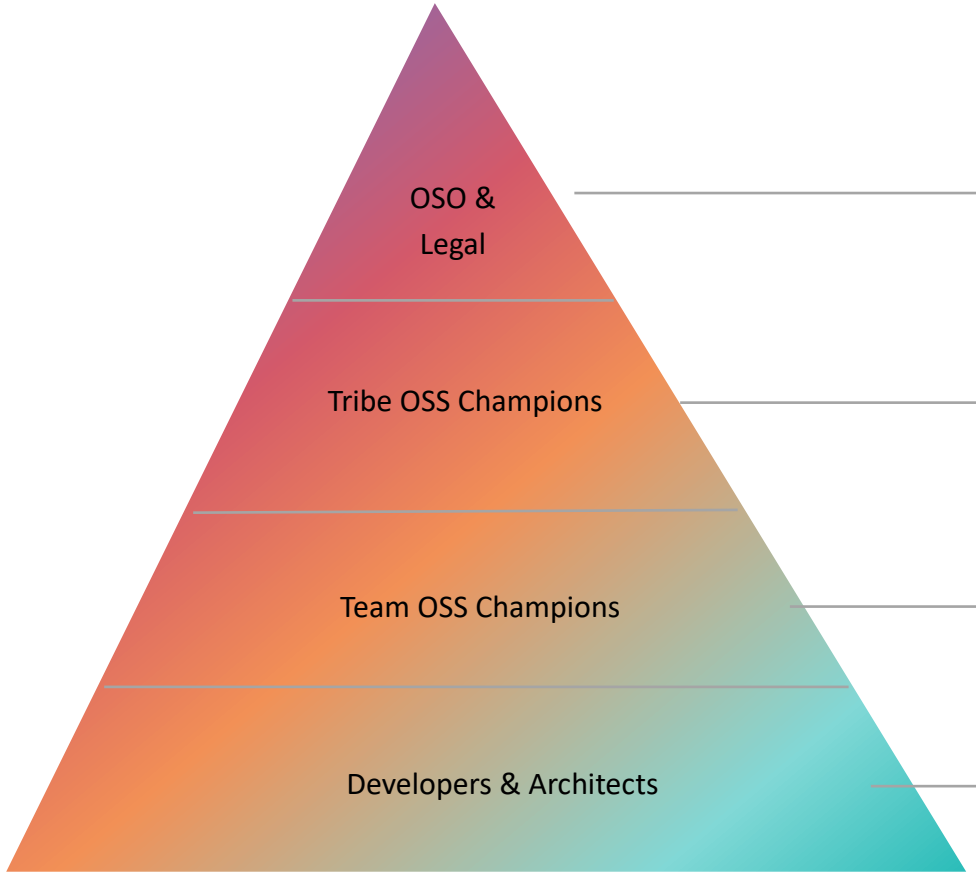
- **Satisfy license obligations.** Your process should be capable of handling Open Source license obligations that arise from your organization's business practices

Benefits of a robust Open Source Compliance program include:

- Increased understanding of the benefits of Open Source and how it impacts your organization
- Increased understanding of the costs and risks associated with using Open Source
- Increased knowledge of available Open Source solutions
- Reduction and management of infringement risk, increased respect of Open Source developers/owners' licensing choices
- Fostering relationships with the Open Source community and Open Source organizations

Source: OpenChain training slides: https://github.com/OpenChain-Project/curriculum

How to scale a small team?



- Defines & deploys Open Source strategy, policy and processes
- Collaborates with the Open Source Community
- Supports champions by providing trainings & guidance
- Responsible for integrates/seamless developer experience
- Final line of support for Open Source

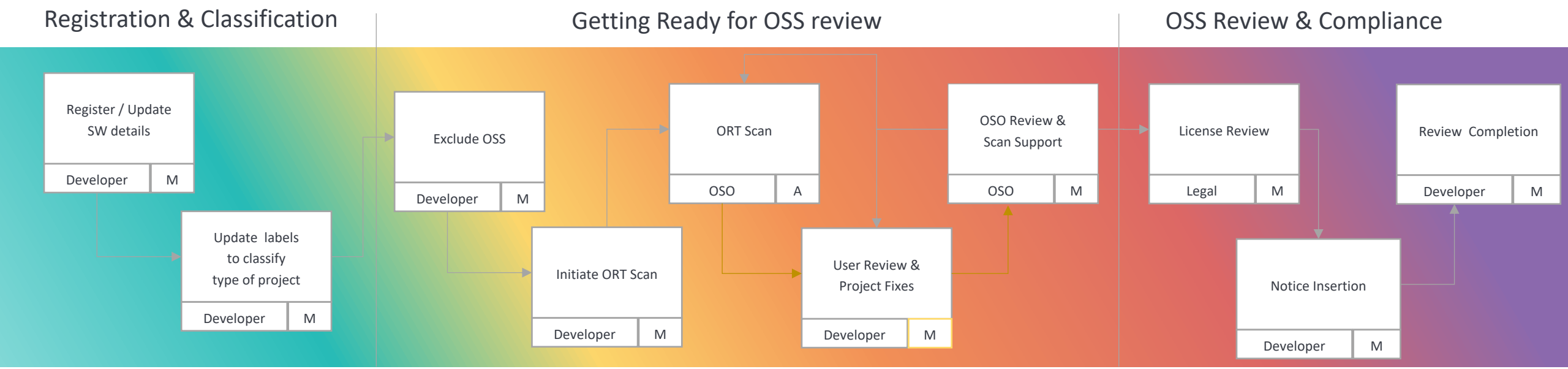
- 2nd line of support for Open Source within the tribe
- Elevate tribe knowledge on Open Source & Engineering best practices
- Promote Open Source culture amongst the tribe
- Act as cross organizational glue

- 1st line of support for Open Source within the teams
- Monitor compliance for the team

- Responsible for compliant products
- Contribute back to the community

Process Workflow

M = Manual
A = Automated



OK /NOT OK = product context + code context + license context + …

What is released to customers? Artifact, service or website?

What does the contract say?

Source code, docs, example, test or build tools?

How is it included? Which scope? Linking?

Did we change the code?

What are the licenses and resulting obligations?

Patents? Freedom to operate?

Created by us or FOSS community?

What information do you need to gather?

OPENCHAIN

When analyzing Open Source usage, collect information about the identity of the Open Source component, its origin, and how the Open Source component will be used. This may include:

• Package name • Status of the community around the package (activity, diverse membership, responsiveness) • Version • Download or source code URL • Copyright owner • License and License URL • Attribution and other notices and URLs • Description of modifications intended to be made	• List of dependencies • Intended use in your product • First product release that will include the package • Location where the source code will be maintained • Possible previous approvals in another context • If from an external vendor: • Development team's point of contact • Copyright notices, attribution, source code for vendor modifications if needed to satisfy license obligations

Source: OpenChain training slides: https://github.com/OpenChain-Project/curriculum

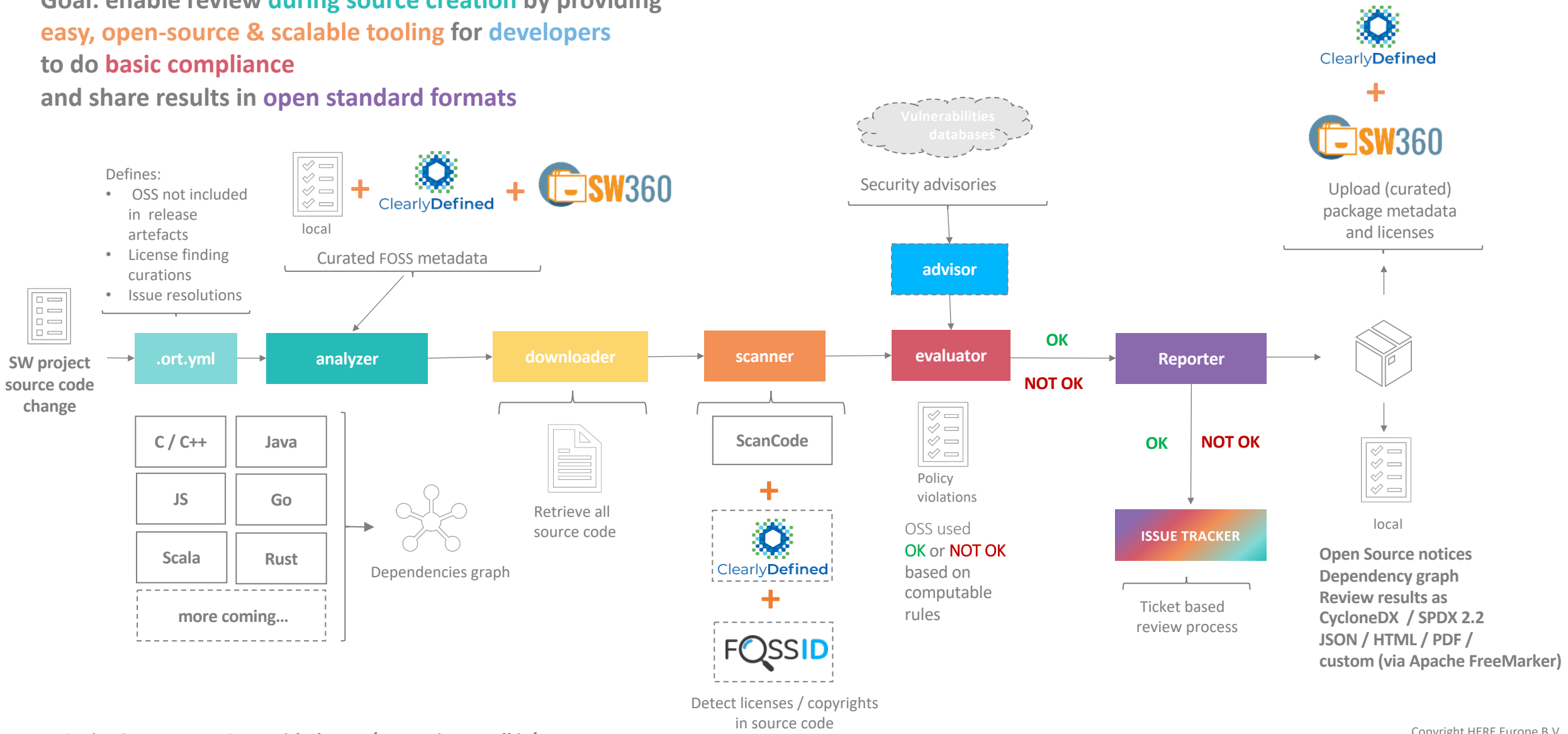
OSS Review Toolkit (Q4 2020)

LEGEND

built

under development

Goal: enable review during source creation by providing easy, open-source & scalable tooling for developers to do basic compliance and share results in open standard formats



Join the ORT community at **github.com/oss-review-toolkit/ort**

OSS Review Toolkit (Q4 2020)

Features:

- License scanning

  Identifies copyrights and licenses by wrapping existing license / copyright scanners like ScanCode to detect findings in local source code directories.

- Best practices / company standards scanning

  Align software projects across the organization.

- Policy violations rule engine

  Perform highly customizable policy checks against scan results

- Software Bill of Materials / Notices

  Generate CycloneDX, SPDX 2.2 files, plain text open source notices or your custom result files (via Apache FreeMarker template)

- Dev Ops integration

  Designed from the beginning for a CI/CD world (Jenkins template available plus soon Azure DevOps and GitLab)

- Security scanning (work in progress)

  Integrations with OSS security vulnerabilities data feeds from various vendors (Nexus IQ supported, VulnerableCode, OSS Index under discussion).

- Source code scanning (work in progress)

  Working on partnerships with vendors (FossID e.a.) to develop integrations to identify published origin of source code and other files

Collected Information

- Package name
- Version
- Source code repository URL
- Source and binary artifacts
- Copyright owner
- License and License URL
- Attribution and other notices and URLs
- List / tree of dependencies
- Location where the source code will be maintained

Questions? Interested in collaborating? Chat with us using the ort-talk Slack channel, see **github.com/oss-review-toolkit/ort**

OSS Review Toolkit

Hands-on Demo

- Project update
- Handling large scan results using ort helper cli
- How to add package metadata to code using SPDX manifests
- How to write context specific policy rules using labels

Lessons Learned (2020 additions)

Organizational

- Use a ‘Drive Down, Shift Left’ approach for roll-out across an organization
- Open source compliance solutions and collaboration enable a small team to scale

Process

- Policy rules change with your changes in your software and the community
- Use automated context specific documentation to help users fix their compliance issues themselves
- Reuse existing version control and CI systems in org where possible

Tools

- Most commercial compliance vendors don’t understand the challenges of license compliance / OSPOs

For 2019 lesson learned, see **Starting and Scaling an Open Source Office**

Thank you　ありがとうございました

Thomas Steenbergen
HERE Open Source Office

thomas.steenbergen@here.com
@tsteenbe
linkedin.com/in/tsteenbe

OSS Review Toolkit

https://github.com/oss-review-toolkit/ort
Starting and Scaling an Open Source Office
ORT Slack

Related OSS Projects

https://oss-compliance-tooling.org
https://clearlydefined.io
https://spdx.org
https://www.openchainproject.org
https://www.doubleopen.org
https://www.eclipse.org/sw360