Standardising the Open Source compliance processes

EOLE, Paris, December 2018

The background

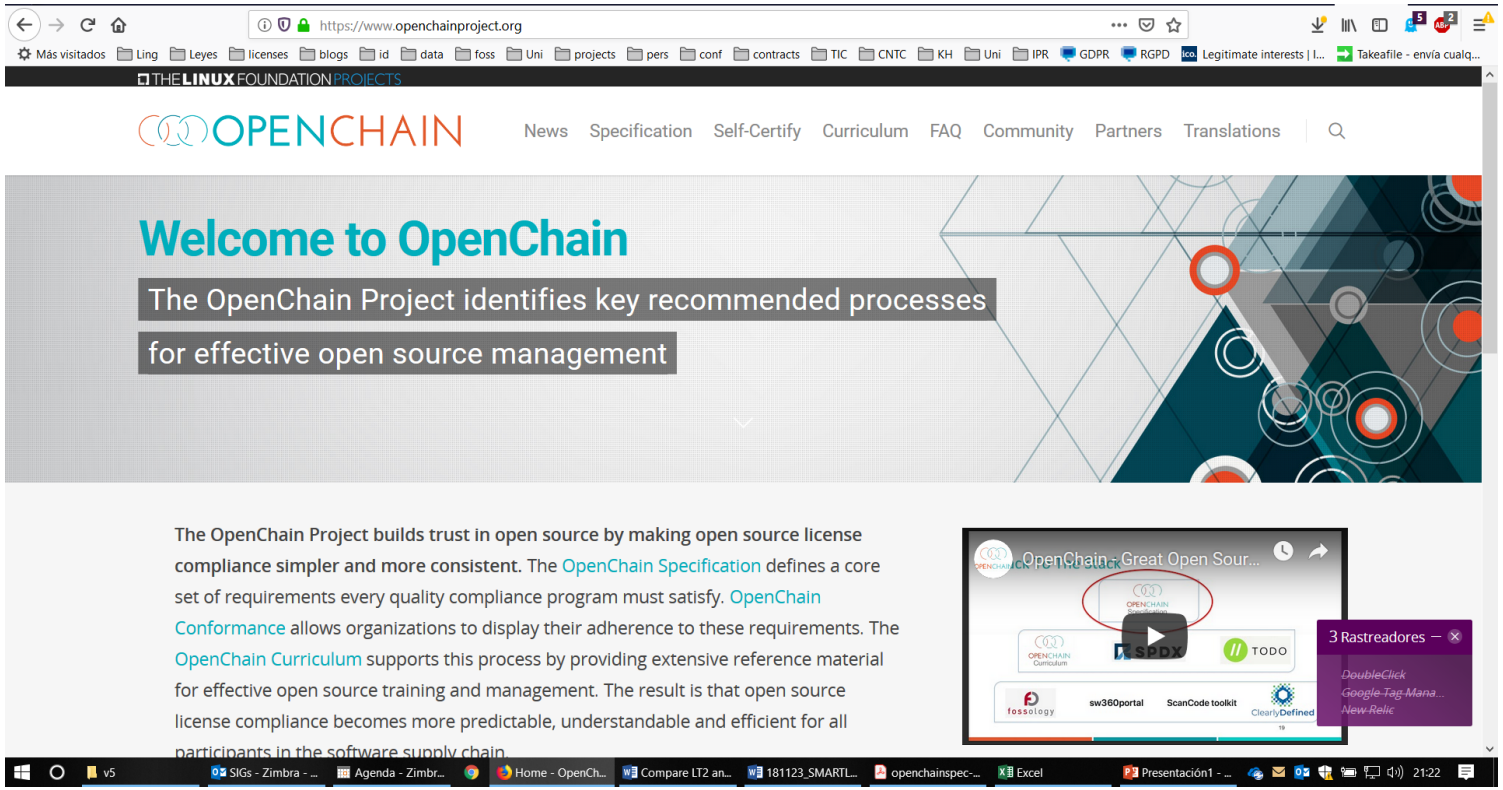
- We all use open source software
- We know it has different licenses
- We know we have to comply with them: attribution and source code
- We have tools for discovering the licenses or do it manually
- We have ideas about compatibility tests, linking, packaging, …

→Question 1: How do we put all this together efficiently?

→Question 2: In a multi-party context like a supply chain?

→Question 3: So that the work is not done repeatedly?

OpenChain Project addresses the question of “how do I trust open source compliance in my supply chain?”



Goals: open source compliance

- Develop an overarching **standard** to describe what organizations could and should do to address open source compliance efficiently gained momentum until the formal project was born.
- Identify **key recommended processes** for effective open source management.
- Build **trust** by having organizations conformant with the OpenChain Specification.

→ reduce bottlenecks and risk when using third-party code to make open source license compliance simple and consistent across the supply chain.

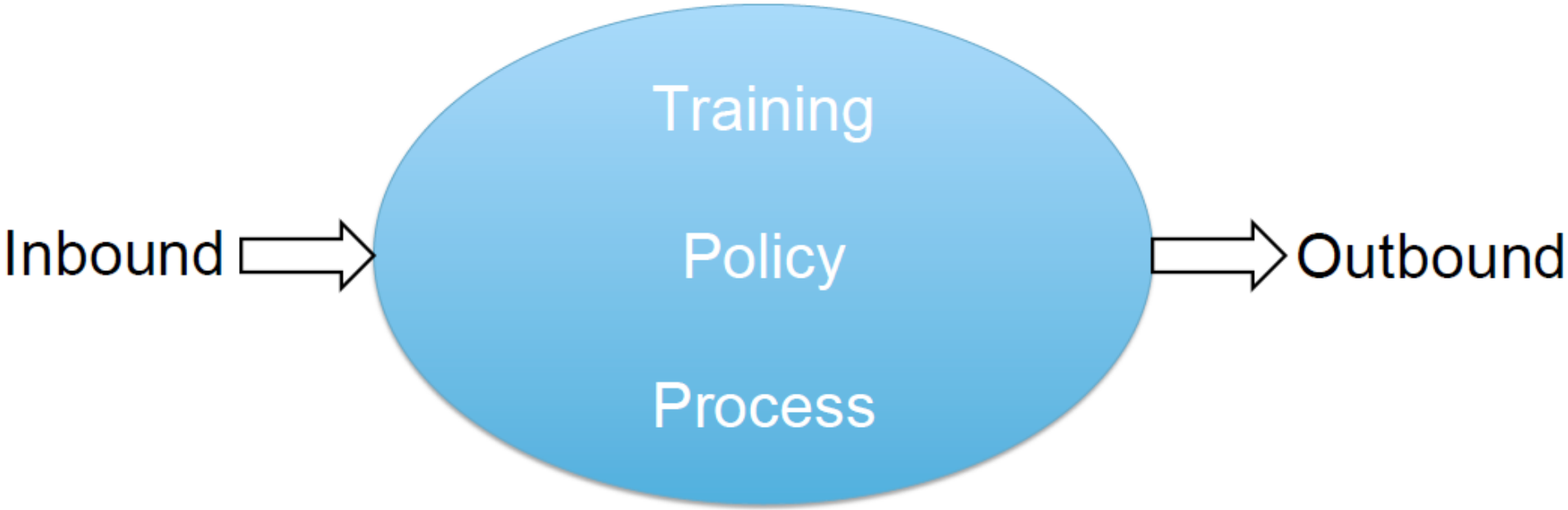
Main Pillars

The OpenChain Project has three pillars.

- The OpenChain Specification defines a core set of requirements every quality compliance program must satisfy.
- OpenChain Conformance allows organizations to check and display their adherence to these requirements.
- The OpenChain Curriculum provides the educational foundation for open source processes and solutions, while meeting a key requirement of the OpenChain Specification.

OpenChain Specification

- At www.openchainproject.org/spec
- Sets out the requirements to comply with



OpenChain Specification

- 6 Chapters
  1. “Program Foundation” – setting a FOSS Policy and Competences
  2. “Roles and Responsibilities” – appointing compliance staff, liaison,
  3. “Review” – creating FOSS component bill of materials and analysis
  4. “Compliance Artefacts” – creating and managing compliance items
  5. “Engagement” – contributing to FOSS projects
  6. “Conformance” – verifying conformance with the standard

OpenChain Conformance

- Check your entity complies with the specification
- Check out https://www.openchainproject.org/conformance

▸ G1: Know Your FOSS Responsibilities		0 answered out of 8
▸ G2: Assign Responsibility for Achieving Compliance		0 answered out of 7
▾ G3: Review and Approve FOSS Content		0 answered out of 3

#	Question	Answer	Spec Ref
3.a:	Do you have a documented procedure for identifying, tracking and archiving information about the collection of FOSS components from which a Supplied Software release is comprised?	Yes | No	3.1.1
3.b:	Do you have FOSS component records for each Supplied Software release which demonstrates the documented procedure was properly followed?	Yes | No	3.1.2
3.c:	Have you implemented a procedure that handles at least the following common FOSS license use cases for the FOSS components of each supplied Supplied Software release?		3.2.1

OpenChain Curriculum

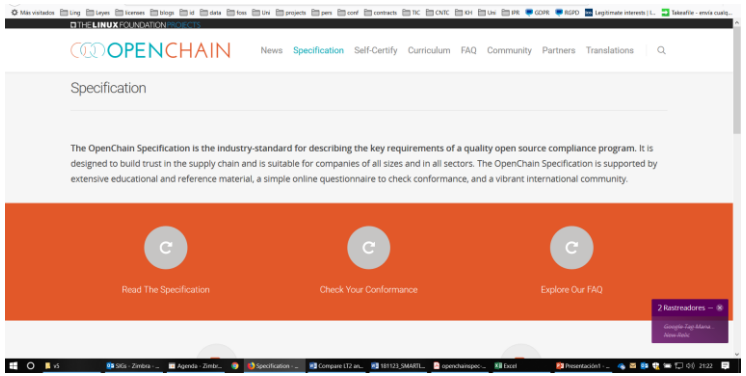
- https://www.openchainproject.org/curriculum
- Started off as a single set of slides for training
- Expanded into a repository of useful information
  - Already contains checklists, flowcharts, guides
  - Continuous ongoing discussions for more
  - Additional content is always welcome!
- Practical info: work is being done/tracked on GitHub
  - Translations are on their own repositories
- Anyone can contribute!

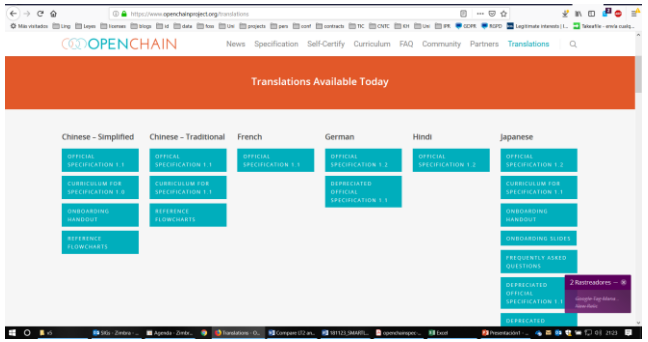
OC curriculum - Contents

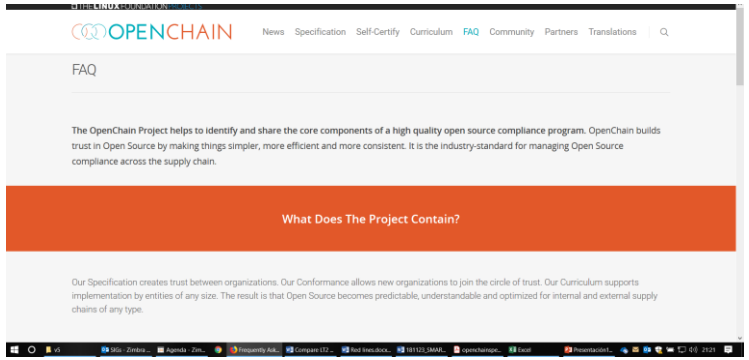
1. What is Intellectual Property?
2. Introduction to FOSS Licenses
3. Introduction to FOSS Compliance
4. Key Software Concepts for FOSS Review
5. Running a FOSS Review
6. End to End Compliance Management (Example Process)
7. Avoiding Compliance Pitfalls
8. Developer Guidelines

OpenChain stuff

- Benefits https://www.openchainproject.org/news/2017/11/29/the-benefits-of-the-openchain-project-in-one-page
- FAQS - https://www.openchainproject.org/faq
- Documents and code: https://github.com/OpenChain-Project
- App: https://certification.openchainproject.org/

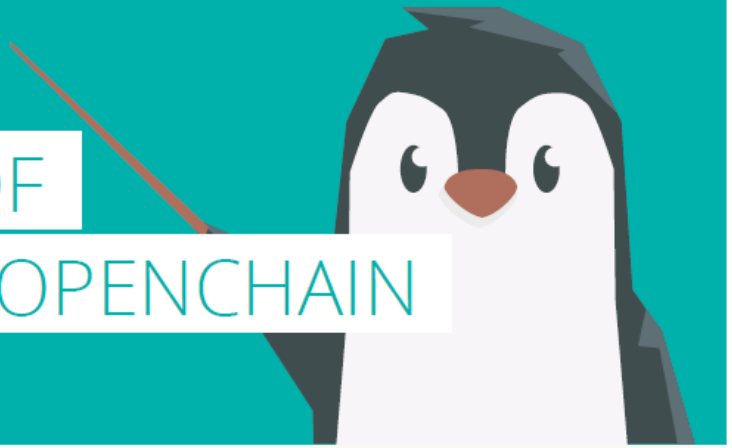






OPENCHAIN

BENEFITS OF ADOPTING OPENCHAIN



1. **OpenChain makes Free and Open-Source Software (FOSS) more accessible to your developers**

   OpenChain provides a framework for shared, compliant use of FOSS. Conforming companies create an environment that supports use of FOSS internally and sharing of FOSS with partners.

2. **OpenChain reduces overall compliance effort, saving time and legal and engineering resources**

   OpenChain allows companies in a supply chain to work together toward FOSS compliance and provides a consistent standard to which all must perform. By contrast, in a typical supply chain, each member of the chain has to perform FOSS compliance for software of others in the chain, wasting time and resources in a duplication of effort.

3. **OpenChain may be adapted to your existing systems**

   OpenChain allows you to choose your own processes to meet its requirements. OpenChain provides resources that help you design new processes from the ground up, or you

SUPPORTING YOUR ENTIRE TEAM:

Legal & Compliance

- Establishes one standard for all members in the supply chain
- Increases license compliance and awareness across the supply chain
- Provides resources to educate vendors, suppliers and other partners on FOSS compliance

Procurement

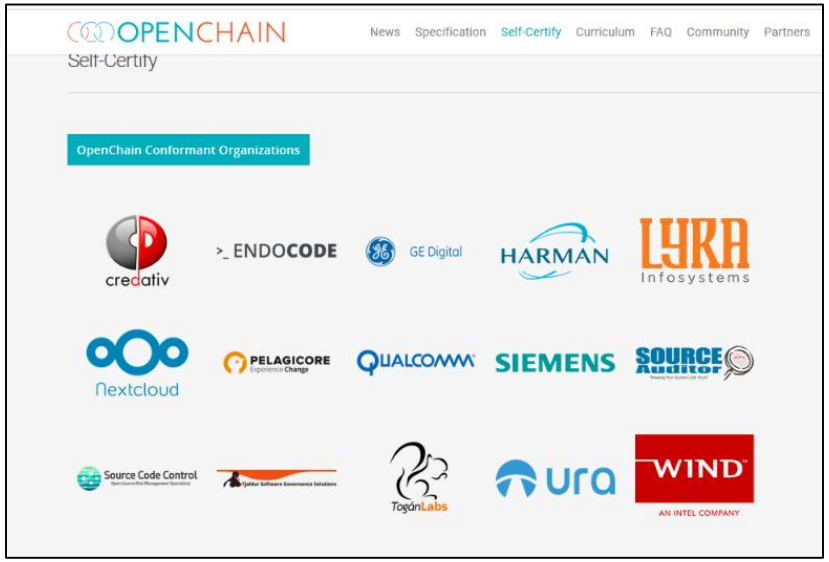
- Simplifies vendor standards in contracting
- Provides a stable, widely supported specification

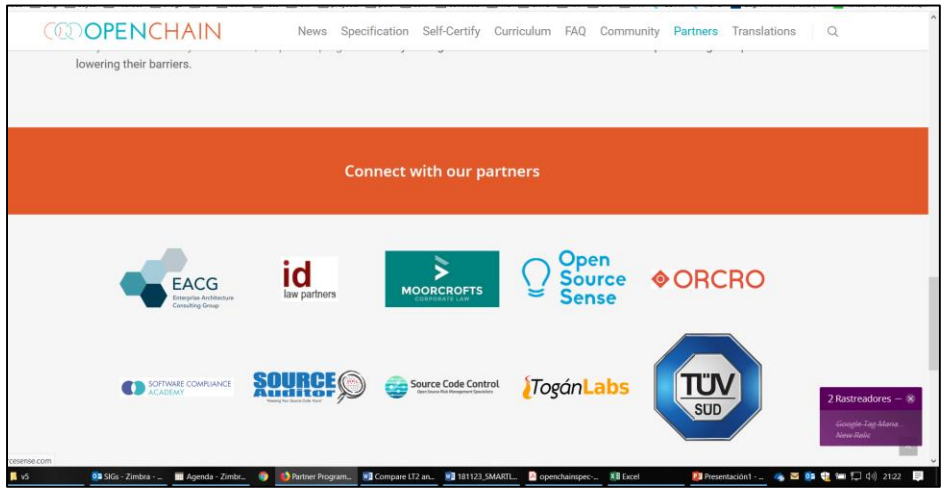
Executive Team

- Reduces overall compliance costs and risks
- Provides a blueprint for cooperation between internal teams

14 Platinum members, 15 compliant companies, 10 Partners

Adobe
Arm
Cisco
Comcast
GitHub
Harman
Hitachi
HPE
Qualcomm
Siemens
Sony
Toyota
Western Digital
Wind River





Ongoing work

- **Specification**: Working on Spec v.2.0
- **Curriculum**: Widening and modularising the materials
  - Adapting to jurisdictions, translating
  - Modularising: focussing on different aspects
- **Onboarding**: disseminating and making it easier to use
  - educating about OpenChain's purpose and benefit and to promote adoption
  - Quick Start Guide (https://www.openchainproject.org/quick-start)

WIDENING THE COMMUNITY!

Thanks for participating

Malcolm Bain

Id law partners / Across Legal

Barcelona

Reasons to Engage

- The **OpenChain Project** is designed to be useful and adoptable for all types of entities in the supply chain. As such, it is important to distill its value proposition for various potential partners. Our volunteer community created a list of five practical reasons to engage:
- **OpenChain makes free and open source software (FOSS) more accessible to your developers.** OpenChain provides a framework for shared, compliant use of FOSS. Conforming companies create an environment that supports use of FOSS internally and sharing of FOSS with partners.
- **OpenChain reduces overall compliance effort, saving time and legal and engineering resources.** OpenChain allows companies in a supply chain to work together toward FOSS compliance and provides a consistent standard to which all must perform. By contrast, in a typical supply chain, each member of the chain has to perform FOSS compliance for software of others in the chain, wasting time and resources in a duplication of effort.
- **OpenChain may be adapted to your existing systems.** OpenChain allows you to choose your own processes to meet its requirements. OpenChain provides resources that help you design new processes from the ground up, or you may choose to use the systems you have in place.
- **OpenChain helps your business teams work together toward a common goal.** OpenChain provides a blueprint for your legal, engineering, and business teams to work together toward FOSS compliance.
- **OpenChain allows you to conform to a stable, community-backed specification.** When you adopt OpenChain, you conform to a stable specification that is widely backed by industry and community participants. OpenChain was developed in an open, collaborative process, with contributors from a wide range of industries across Asia, Europe and North America. OpenChain is being formally adopted by a growing number of both small and larger companies.