



# OPENCHAIN

Great Open Source Compliance For Everyone

OpenChain Project - The Linux Foundation

Available under the [CC Attribution-NoDerivatives 4.0 International license](#).



## Largest Shared Technology Investment

The Linux Foundation supports the creation of sustainable open source ecosystems by providing financial and intellectual resources, infrastructure, services, events, and training. Working together, The Linux Foundation and its projects form the most ambitious and successful investment in the creation of shared technology.



**16B USD**

Estimated development cost of the  
100+ world's leading projects  
hosted at The Linux Foundation



**25,000**

Technologists attend our events  
annually, from more than 4,500  
companies and 85 countries



**1 Million**

Open source professionals have  
enrolled in our free open source  
training courses

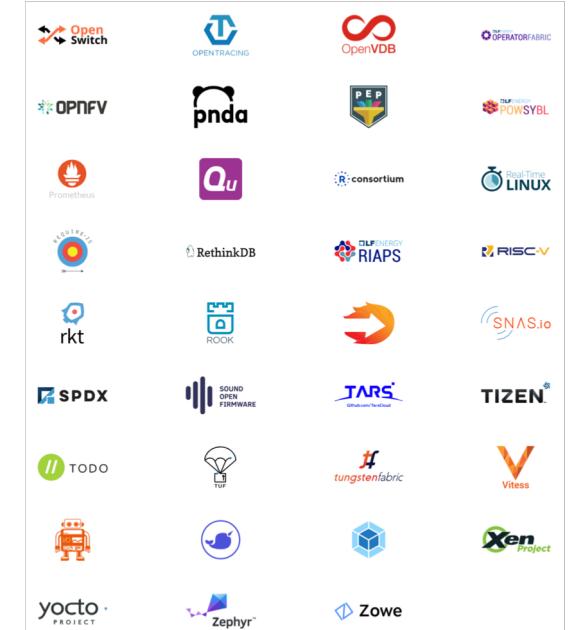
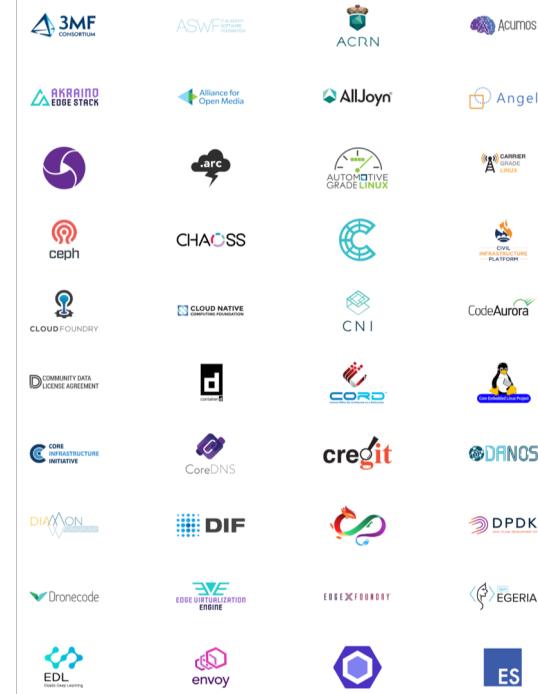
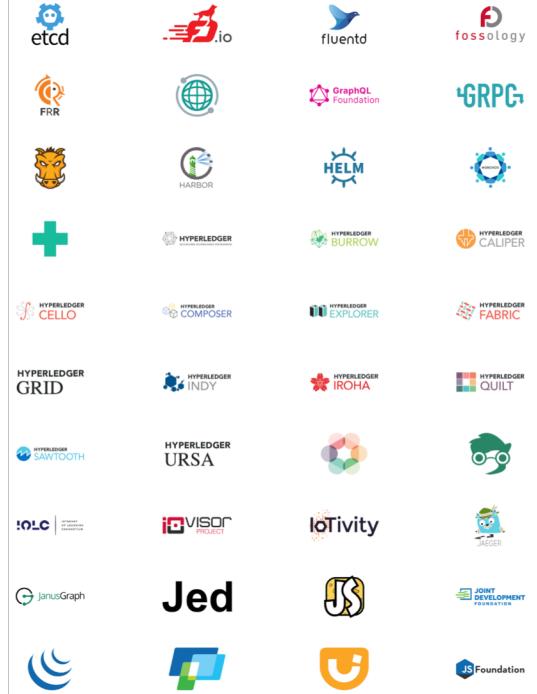
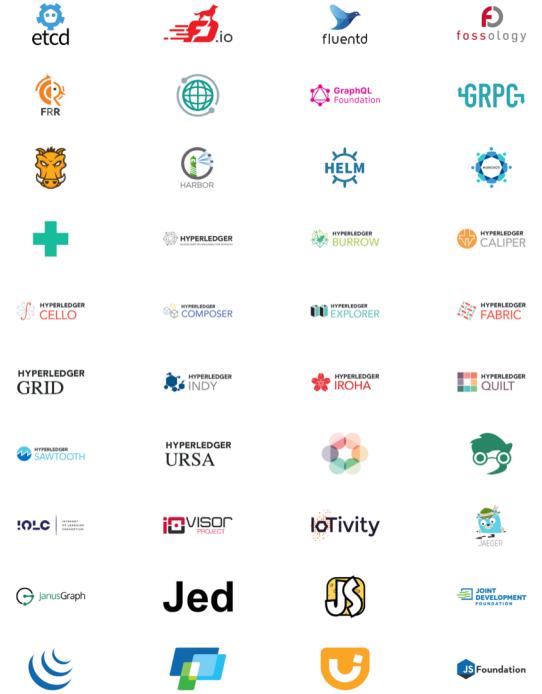


**10 / 10**

Largest cloud service providers are  
Linux Foundation project  
contributors and members



**OPENCHAIN**

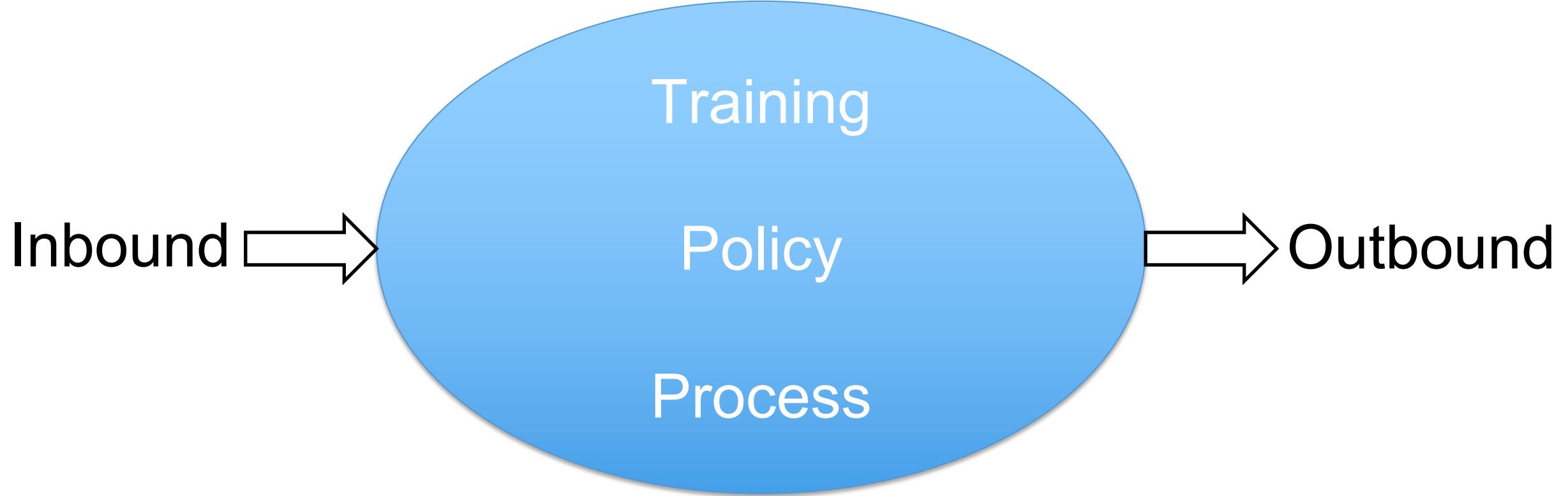


# Compliance – A gateway to access

# How do I trust my open source supply chain?

The OpenChain Project defines the key requirements for a quality compliance program.

**OpenChain is a simple, effective standard for all sizes organizations in all markets.**



**Companies have the flexibility to decide the content of each specific process, policies and training.**

# OpenChain Self Certification Questionnaire

## Specification Version 1.3

[Select Version](#)

► G1: Know Your FOSS Responsibilities	8 answered out of 13
► G2: Assign Responsibility for Achieving Compliance	0 answered out of 7
► G3: Review and Approve FOSS Content	0 answered out of 8
▼ G4: Deliver FOSS Content Documentation and Artifacts	3 answered out of 4
 <input checked="" type="radio"/> Yes <input type="radio"/> No     Do you have a documented procedure that describes a process that ensures the Compliance Artifacts are distributed with Supplied Software as required by the Identified Licenses?	
 <input type="radio"/> Yes <input checked="" type="radio"/> No     Do you archive copies of the Compliance Artifacts of the Supplied Software?	
 <input checked="" type="radio"/> Yes <input type="radio"/> No     Can you easily retrieve the archived copies of the Compliance Artifacts of the Supplied Software?	
<input type="radio"/> Yes <input checked="" type="radio"/> No     Are the copies of the Compliance Artifacts archived for at least as long as the Supplied Software is offered or as required by the Identified Licenses (whichever is longer)?	
► G5: Understand FOSS Community Engagement	0 answered out of 4

If a company can answer “Yes” to each question they are OpenChain Conformant.



Organizations with a publicly announced OpenChain Conformant Program

AB EHR Digital  
Electronic Health Records



>\_ENDOCODE



HITACHI  
Inspire the Next

Interneuron



NODEWEAVER



QUALCOMM

SCANIA

SIEMENS



Source Code Control  
Open Source Risk Management Specialists



the Center for Research and  
Development Hong Kong



TogánLabs



The OpenChain Project provides reference material to help with conformance.

# 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

# Check Your Understanding

- What type of material does copyright law protect?
- What copyright rights are most important for software?
- Can software be subject to a patent?
- What rights does a patent give to the patent owner?
- If you independently develop your own software, is it possible that you might need a copyright license from a third party for that software?  
A patent license?



Reference Training Program  
(PDF Format)



Reference Training Program  
(PowerPoint Format)



Reference Training Program  
(OpenDocument Format)



Compliance Best Practices



Engineering Best Practices



Reuse Best Practices



Basic Compliance Checklist



Conformance Checklist



Reference Tooling Overview  
(PDF Format)



Reference Tooling Overview  
(PowerPoint Format)



Reference Tooling Overview  
(OpenDocument Format)

Platinum Members



facebook

Google



HITACHI  
Inspire the Next



QUALCOMM

SIEMENS

SONY

TOSHIBA

TOYOTA

Uber

Western Digital.

## Community

---



Shane Coughlan  
General Manager

[LinkedIn](#) / [Facebook](#) / [Twitter](#)



Mark Gisi  
Specification Chair

[LinkedIn](#)



Miriam  
Ballhausen  
Conformance Chair

[LinkedIn](#)



Alexios Zavras  
Curriculum Chair

[LinkedIn](#)



Dave Marr  
Governing Board Chair

[LinkedIn](#)

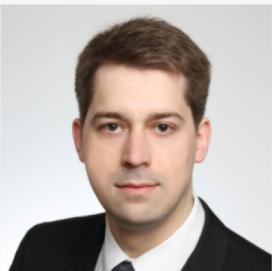


Kelly Williams  
Secretary Emeritus



Catharina  
Maracke  
Strategic Advisor

[LinkedIn](#)



Matija Suklje  
Strategic Advisor

[LinkedIn](#)



Gary O'Neill  
Lead Developer

[LinkedIn](#)



Indira Bhatt  
Community  
Representative

[LinkedIn](#)

# Work Teams supporting OpenChain:

1. Specification - Chaired by Mark Gisi (Wind River)
2. Conformance - Chaired by Miriam Ballhausen (SCA)
3. Curriculum - Chaired by Alexios Zavros (Intel)
4. Onboarding - Chaired by Nathan Kumagai (Qualcomm)

## Join Our Conference Calls

We have a call on the first Monday of each month at 4pm UTC to allow participation for American and European community members.  
We have a call on the third Monday of each month at 12am UTC to allow participation for American and Asian community members.



UberConference



US Call



International Call  
(Code #855 889 3011)

## Join Our Mailing Lists



Main Project Mailing List

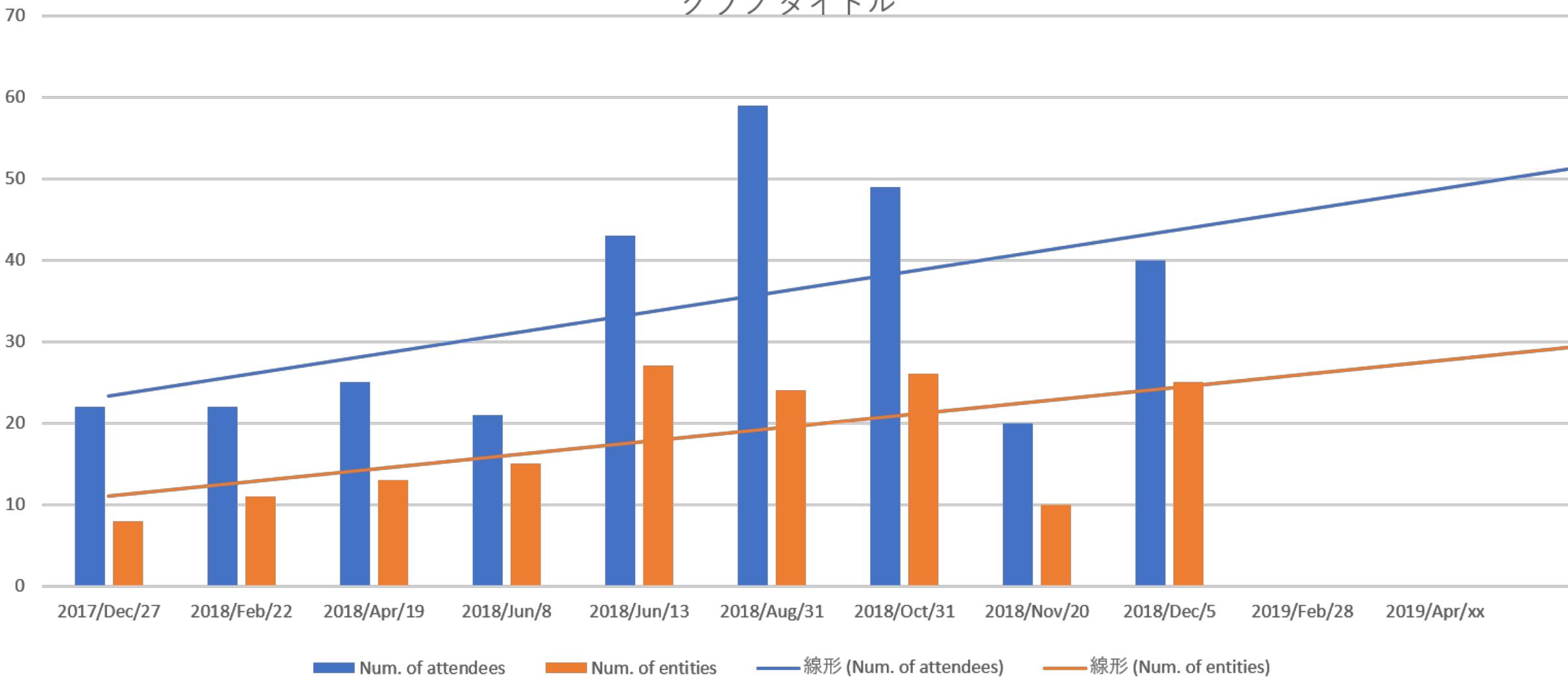


Specification Mailing List

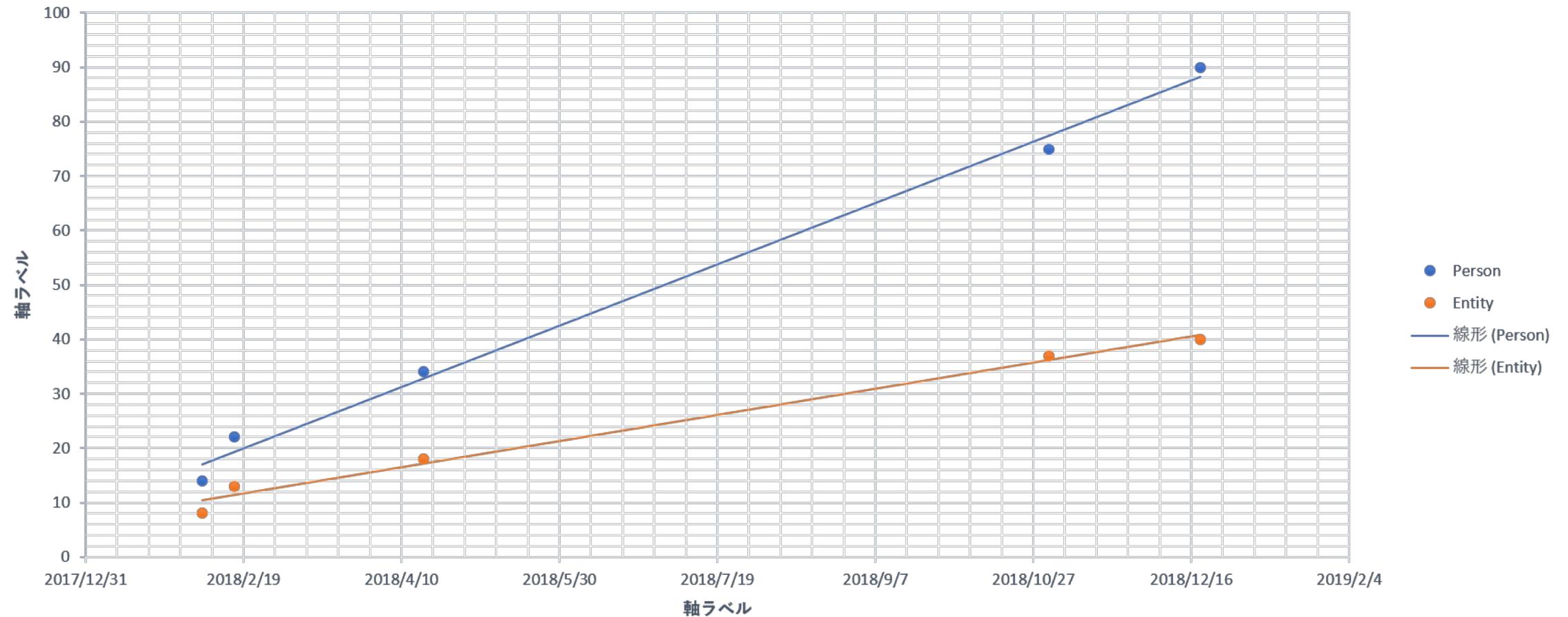
# Recent Progress

1. International Partners - from law firms to certification authorities in Europe, Asia and the Americas
2. Significant new board members like Toshiba, Facebook, Google, Uber and Microsoft
3. A move towards formal standardization via the PAS process for ISO with ETA Q1 2020

グラフ タイトル



# Meetings in Japan



# Japanese Mailing List

# Audited Certification



Page 1 of 1  
TÜV SÜD Product Services GmbH - Institute Study - Maxvorstadtstr. 61 - 80539 Munich - Germany



# What is happening now

OpenChain FAQ 2.0

File Edit View Insert Format Tools Add-ons Help Last edit was made 11 days ago by anonymous

SHARE

100% Title Arial 26 B I U A

OpenChain Questions and Answers 2.0

Release Candidate 2

**Q&A Already Published (we are improving language)**

What is the OpenChain Project?

The OpenChain Project identifies the key requirements of a high quality open source compliance program. It builds trust in open source by making things simpler, more efficient and more consistent. The OpenChain Specification is the industry-standard for managing open source compliance across the supply chain.

How does OpenChain work?

The OpenChain Project maintains a standard designed to create trust between organizations called the OpenChain Specification. We provide online and offline self-certification and extensive reference material to assist with implementation. The result is that open source becomes more predictable, understandable and efficient for internal and external supply chains of any type.

How Is The Project Organized?

The OpenChain Project has four public work teams:

1. The Specification Work Team identifies and publishes the key requirements of a quality open source compliance program.
2. The Conformance Work Team helps companies check that they are adhering to the Specification requirements.
3. The Curriculum Work Team provides reference material to help companies meet the Specification requirements.
4. The Onboarding Work Team creates material to make it easy to understand the OpenChain Project.

There are also three committees for member companies:

1. The Governing Board manages policies or rules and procedures for the Project, fund raising, budgeting and so forth.
2. The Steering Committee develops, manages and updates the OpenChain Compliance Specification.
3. The Outreach Committee designs, develops and executes activities to expand the OpenChain ecosystem.

How does the OpenChain Specification work?

There are four principles that guide the development of the OpenChain Specification:

1. Build trust around the use of open source.
2. Use a "Less is More" approach focused on the key requirements of a quality compliance program.
3. Focus on "what and why" rather than "how and when" to ensure freedom of choice.
4. Be an open development initiative that welcomes all contributions.

Who Conforms To The OpenChain Standard?

We maintain a [list of organizations that have a publicly announced OpenChain Conformant Program](#). The OpenChain standard is primarily focused on the relationship between suppliers and customers, so organizations have the freedom to be conformant without public announcement.

Where can I find the current version of the specification?

Shane Coughlan 4:36 PM Jan 9 Resolve

See below in document for "Questions to be answered" and suggested new format.

Path to Conformance DRAFT

File Edit View Insert Format Tools Add-ons Help Last edit was made yesterday at 9:10 AM by Nathan Kumagai

SHARE

100% Normal text Arial 24 B I U A

## Path to Conformance

We recognize that organizations in our community are at different levels in building their open source compliance processes. We illustrate this process as four levels in the "Path to Conformance."

For each level, we are gathering resources to support our community organization moved through the conformance process.

### Level 1: Gaining awareness of open source compliance

Organizations in this stage may be asking:

- What are open source risk? How can failing to comply with open source obligations impact engineering, business and legal teams?
- How do I communicate the importance of open source compliance to my partners or within my own organization?
- What are the benefits of open source compliance?

Resources currently available include:

1. Checklist Handout - <https://docs.google.com/document/d/1Lfx9mK0ZaZMLZzZ2mjHAqgFdQNuYrCXVnFmgFZdcU/edit?usp=sharing>
2. Awareness Handout (NEW) - <https://docs.google.com/document/d/1YNkIrp0GoB1GLwhQDNzxKjOTnFESEdRGtHF5f30QXk/edit?usp=sharing>

Nathan Kumagai 9:10 AM Yesterday Resolve

Note: In each case we will link in the various language versions

### Level 2: Understanding how OpenChain addresses compliance risks

Organizations in this stage may be asking:

- What are the benefits of OpenChain conformance?
- What are key elements of the OpenChain project?
- What are costs of conformance?
- What are requirements for joining the community? For obtaining/implementing the specification?

Resources currently available include:

1. OpenChain Overview - <https://docs.google.com/document/d/1ctovs6PpVrignQSqSXFaMzHEgK7D8Tv40te4yPVK8cg/edit?usp=sharing>



## 3) Requirements

### 1.0 Program Foundation

#### 1.1 Policy

A written Open Source policy exists that governs Open Source license compliance of the Supplied Software distribution. The policy must be internally communicated.

**Verification Material(s):**

- 1.1.1 A documented Open Source policy.
- 1.1.2 A documented procedure that makes Software Staff aware of the existence of the Open Source policy (e.g., via training, internal wiki, or other practical communication method).

**Rationale:**

To ensure steps are taken to create, record and make Software Staff aware of the existence of a Open Source policy. Although no requirements are provided here on what should be included in the policy, other sections may impose requirements on the policy.

#### 1.2 Competence

**The organization shall:**

- Identify the roles and the corresponding responsibilities of those roles that affects the performance and effectiveness of the Program;
- Determine the necessary competence of person(s) fulfilling each role
- Ensure that these persons are competent on the basis of appropriate education, training, and/or experience;
- Where applicable, take actions to acquire the necessary competence
- Retain appropriate documented information as evidence of competence

**Verification Material(s):**

- 
- 1.2.1 A documented list of roles with corresponding responsibilities for the different participants in the Open Source compliance program;
- 1.2.2 A documented that identifies the competencies for each role
- 1.2.3 Documented evidence of assessed competence for each program participant

**Rationale:**

To ensure that the program participants have obtain a sufficient level of competence for their respected roles and responsibilities.

#### 1.3 Awareness

**The organization shall ensure that persons doing work are aware of:**

- a) The Open Source policy;

## 3) Requirements

### Goal 1.0: Know Your Open-Source Responsibilities

#### 1.1 Policy

A written Open Source policy exists that governs Open Source license compliance of the Supplied Software distribution. The policy must be internally communicated.

**Verification Material(s):**

- 1.1.1 A documented Open Source policy.
- 1.1.2 A documented procedure that makes Software Staff aware of the existence of the Open Source policy (e.g., via training, internal wiki, or other practical communication method).

**Rationale:**

To ensure steps are taken to create, record and make Software Staff aware of the existence of a Open Source policy. Although no requirements are provided here on what should be included in the policy, other sections may impose requirements on the policy.

**Mandatory Open-Source training for all Software Staff exists such that:**

The training, at a minimum, covers the following topics:

The Open-Source policy and where to find a copy;

Basics of Intellectual Property law pertaining to Open-Source and Open-Source licenses;

Open-Source licensing concepts (including the concepts of permissive and copyleft licenses);

Open-Source project licensing models;

Software Staff roles and responsibilities pertaining to Open-Source compliance specifically and the Open-Source policy in general; and

Process for identifying, recording and/or tracking of Open-Source components contained in Supplied Software.

Software Staff must have completed Open-Source training within the last 24 months to be considered current ("Currently Trained"). A test may be used to allow Software Staff to satisfy the training requirement.

#### 1.2 Competence

**The organization shall:**

- Identify the roles and the corresponding responsibilities of those roles that affects the performance and effectiveness of the Program;
- Determine the necessary competence of person(s) fulfilling each role
- Ensure that these persons are competent on the basis of appropriate education, training, and/or experience;
- Where applicable, take actions to acquire the necessary competence
- Retain appropriate documented information as evidence of competence

**Verification Material(s):**

## OpenChain Specification 1.2



German



Hindi



Japanese

## OpenChain Specification 1.1



Chinese (Simplified)



Chinese (Traditional)



French



German



Japanese



Korean



Portuguese



Spanish

Code

Issues 1

Pull requests 0

Projects 0

Wiki

Insights

Settings

Branch: master ▾

Specification-Translation-IT / final\_it.md

Find file Copy path

**kappapiana** more merge, screwed up a bit, earlier on

04e6a64 on Nov 16, 2017

1 contributor

394 lines (289 sloc) | 19.2 KB

Raw

Blame

History



## Contents

Copyright © 2016-2017 Linux Foundation. Questo documento è distribuito con licenza Creative Commons Attribuzione 4.0 Internazionale (CC-BY 4.0) . Una copia della licenza è reperibile presso <https://creativecommons.org/licenses/by/4.0/>.

# Introduzione

L'OpenChain Initiative cominciò nel 2013 quando un gruppo di operatori impegnati nella filiera di approvvigionamento del software open source osservò l'insorgenza di due tendenze:

- esistevano significative similitudini tra organizzazioni con programmi maturi di conformità open source; e
- permaneva un ampio numero di organizzazioni che scambiavano software con programmi meno evoluti.

Dalla seconda osservazione scaturiva una mancanza di fiducia nella uniformità e qualità dei risultati in termini di conformità che si accompagnavano al software così scambiato. Come conseguenza, a ogni passaggio nella catena di fornitura, le organizzazioni a valle si trovavano frequentemente a compiere nuovamente gli sforzi di conformità già eseguiti da altre organizzazioni a monte.

E fu formato un gruppo di studio al fine di considerare se potesse essere creato un programma di specifiche standardizzate



## OpenChain Specification 1.2

### 1) 제 1 절 소개

OpenChain Initiative는 2013년, 소프트웨어 공급망 오픈소스 전문가 그룹이 다음과 같은 두 가지 새로운 패턴을 관찰하면서 시작되었다.: 1) 성숙한 오픈소스 커뮤니티 프로그램이 있는 조직 간에는 중요한 절차적 유사성이 존재함; 2) 덜 발달된 프로그램으로 소프트웨어를 거래하는 조직도 여전히 많이 존재하고 있음. 여기에서 두 번째 패턴은 소프트웨어 거래 시 수반하는 커뮤니티 결과물의 일관성 및 품질에 대한 신뢰가 결여되는 결과를 가져왔다. 결과적으로 소프트웨어 공급망 내 각 단계에서의 하위 조직은 상위 조직에서 이미 수행한 커뮤니티 작업을 다시 수행하는 일이 자주 발생하게 되었다.

이에 다음의 역할을 하는 표준적 프로그램 설명서가 제작될 수 있는지 검토하기 위해 스터디 그룹이 구성되었다: i) 업계에서 공유되는 오픈소스 커뮤니티 정보의 품질과 일관성 향상; ii) 커뮤니티 재작업으로 인해 발생하는 높은 오픈소스 관련 거래 비용의 절감. 이 스터디 그룹은 워크 그룹으로 발전하였으며, 2016년 4월에는 Linux Foundation Collaborative Project로 정식 조직되었다.

OpenChain Initiative의 비전과 사명은 다음과 같다:

- **비전:** 신뢰할 수 있고 일관된 커뮤니티 정보와 함께 Free/Open Source Software(FOSS)를 제공하는 소프트웨어 공급망
- **사명:** 소프트웨어 공급망 참가자를 위해, FOSS의 효과적인 관리를 위한 요구를 수립하여 요구 및 부수적인 관련 사항을 소프트웨어 공급망, 오픈소스 커뮤니티 및 학계의 대표들이 공동으로 그리고 공개적으로 개발할 수 있도록 한다.

비전과 사명에 따라 이 설명서 일련의 요구를 정의하고, 이 요구를 충족하는 오픈소스 프로그램이라면 충분한 수준의 품질, 일관성 및 완전성을 달성했을 가능성을 높일 것이다. 다만, 설명서의 모든 요구를 만족하는 프로그램이라도 완전한 커뮤니티가 보장되는 것은 아니다. 이 요구는 프로그램이 OpenChain을 준수하는 것으로 인정하기 위해 충족해야 하는 기본 수준(최소) 요구들을 의미한다. 이 설명서는 "어떻게"와 "언제"에 대한 고려가 아닌 커뮤니티 프로그램의 "무엇"과 "왜"에 대해 초점을 맞추고 있다. 이는 서로 다른 조직이 각자의 목적에 가장 잘 부합하도록 정책과 프로세스를 조정할 수 있게 하는 실질적인 유연성을 보장한다.

제 2 절에서는 설명서 전체에 걸쳐서 사용되는 주요 용어의 정의를 소개한다. 제 3 절에서는 각 설명서 요구를 나타내는데, 각 요구에 대해 하나 혹은 그 이상의 검증 자료를 제시한다. 이들은 어떤 요구가 충족된 것으로 인정되기 위해 필요한 증거이다. 만약 어떤 프로그램이 모든 요구를 충족한다면, 그 프로그램은 이 설명서 버전 1.2에 따라 OpenChain 준수 프로그램으로 인정될 것이다. 검증 자료는 공개용으로 작성된 것은 아니지만, 준수를 인증하기 위해 NDA(비공개합의) 하에서 또는 OpenChain 조직의 개별적 요청에 따라 제공될 수 있다.



이 슬라이드는 OpenChain Curriculum 공식 번역본입니다.  
공동번역: 박종백/법무법인태평양/jb.park@bkl.co.kr, 장학성/LG전자/hakssung@gmail.com

### OpenChain 설명서 1.2을 위한 FOSS 교육 참조 슬라이드

CC0-1.0에 따라 제공됨  
제한없이 이 슬라이드를 사용, 수정 및 공유할 수 있음.  
보증 없이 제공됨.

이 슬라이드는 미국 법률을 따름. 법적 관할국에 따라 법적 요구 사항이 달라질 수 있음. 이 슬라이드를 커뮤니티 프로그램의 일부로 사용할 때는 이를 고려하여야 함.

이 슬라이드에는 법률 자문이 포함되어 있지 않습니다.

### OpenChain 커리큘럼이란?

- OpenChain 프로젝트는 FOSS(Free and Open Source Software) 커뮤니티 프로그램의 핵심 구성 요소를 식별하고 공유하는데 도움이 된다.
- OpenChain 프로젝트의 핵심은 설명서(Specification)이다. 이는 FOSS 커뮤니티 프로그램이 충족해야 하는 핵심 요구 사항을 식별하고 공표한다.
- OpenChain 커리큘럼은 자유롭게 사용할 수 있는 교육 자료를 제공함으로 설명서를 지원한다.
- 이 슬라이드는 회사들이 설명서 1.2의 요구 사항을 충족하는 데 도움이 된다. 또한, 일반 커뮤니티 프로그램 교육에도 사용할 수 있다.

자세한 내용 참조: <https://www.openchainproject.org>

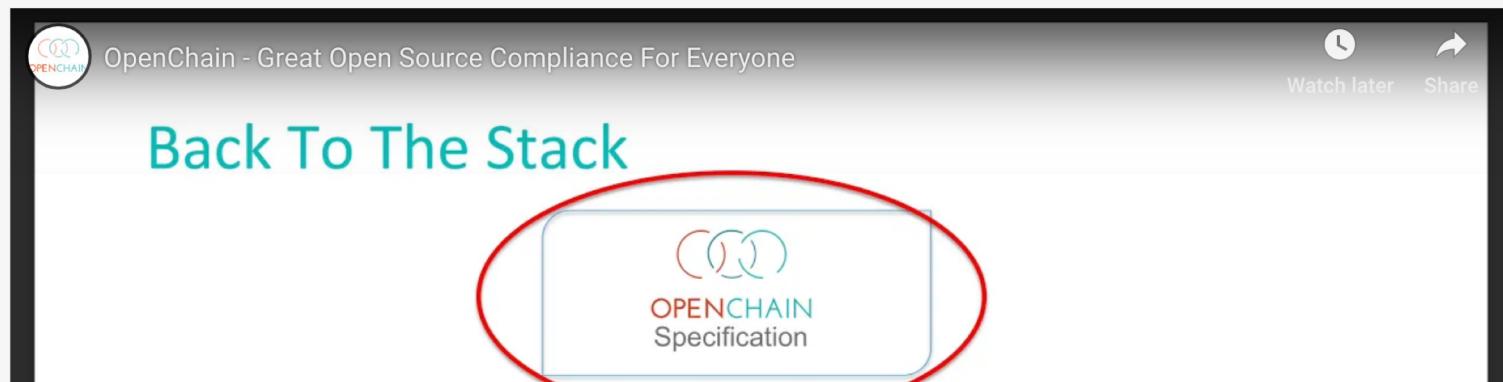


# Welcome to OpenChain

The OpenChain Project identifies key recommended processes  
for effective open source management



OpenChainプロジェクトは、オープンソース コンプライアンスをより簡単に、より一貫性のあるものにすることで、オープンソースへの信頼を築いています。OpenChain仕様では、すべての品質適合プログラムが満足すべき中核となる要件を定義しています。OpenChain適合によって、組織が要件に適合していることを示すことができます。OpenChainカリキュラムでは、効果的なオープンソースのトレーニングやマネージメントを行うための幅広い参考資料を提供することで、このプロセスをサポートします。その結果、オープンソース・ライセンス・コンプライアنسがソフトウェアサプライチェーンの中にいる者にとって、より予測可能でわかりやすく、効率的なものになります。。



# Be part of this

Join the community:

<https://www.openchainproject.org/community>

Self-certify an organization:

<https://certification.openchainproject.org>



coughlan@linux.com