OpenChain 台灣社群聚會：首發工作坊

OpenChain 2.0 Specification in a Nutshell

SZ Lin (林上智)

Software R&D Engineer, Software Development Dept. / 軟體工程師

Debian Developer / Debian 開發者

OpenChain Project Governing Board Member / OpenChain Project 治理委員

12th August, 2020

MOXA®

Reliable Networks ▲ Sincere Service

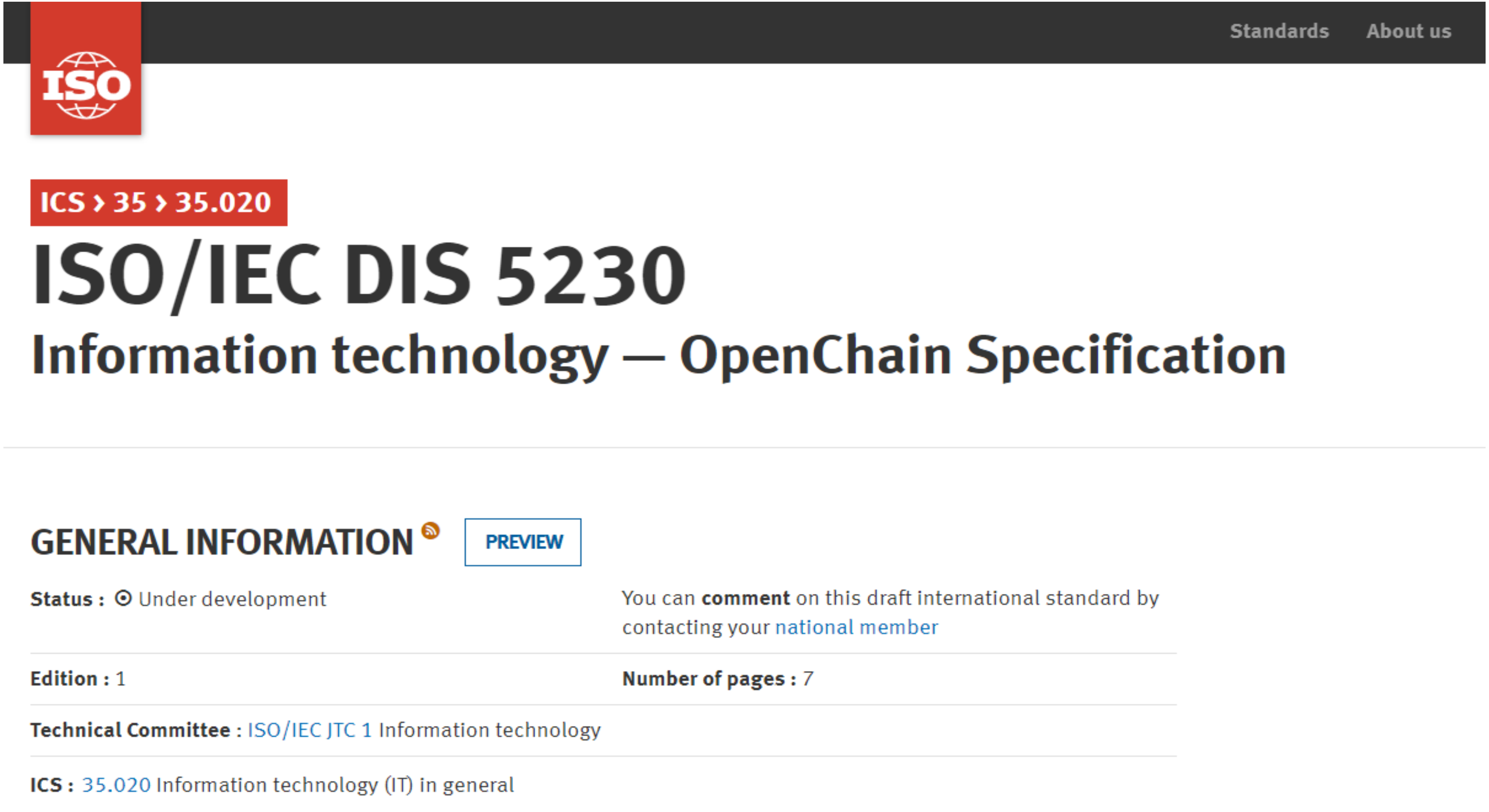
OpenChain 規範定義開源授權合規方案主要要件以確保其品質。

目的是為了提供建立信任的基準讓組織間能夠交換由開源軟體組成的軟體解決方案。

OpenChain 一致性方案可以涵蓋單個產品線或整個組織。

不同的組織能選擇他們的政策及進程以適切符合他們的規模，目標以及範圍

審核稽證不需要公開，組織可基於保密協議 （NDA）選擇將其提供給他人。



ICS › 35 › 35.020

ISO/IEC DIS 5230

Information technology — OpenChain Specification

GENERAL INFORMATION

Status : ⊙ Under development

You can **comment** on this draft international standard by contacting your national member

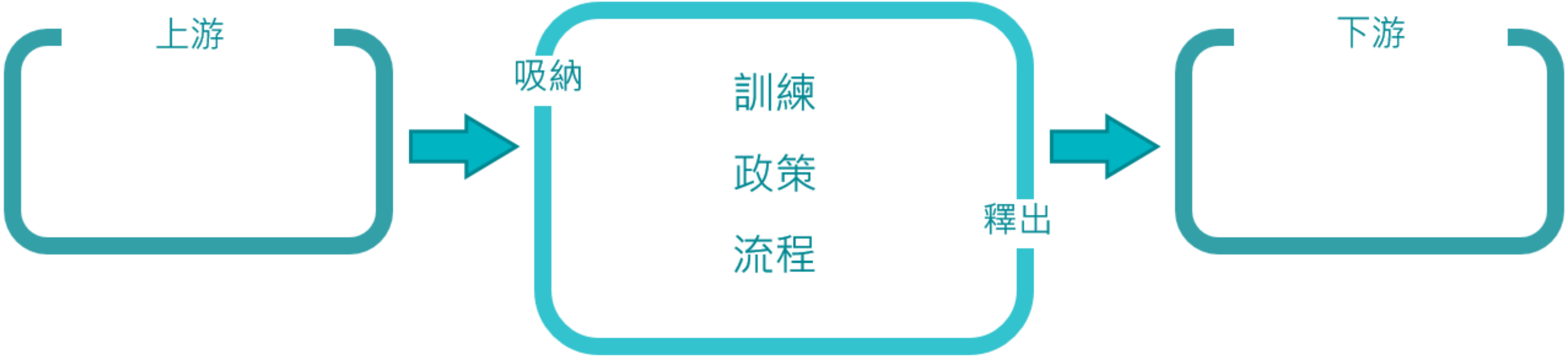
Edition : 1

Number of pages : 7

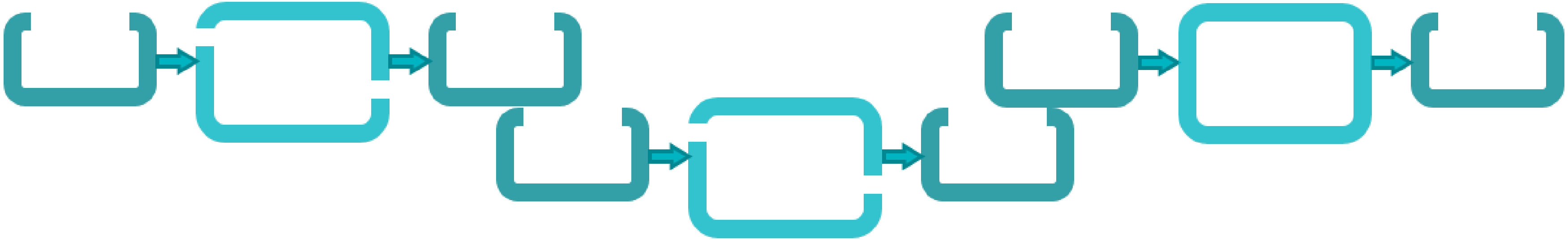
Technical Committee : ISO/IEC JTC 1 Information technology

ICS : 35.020 Information technology (IT) in general

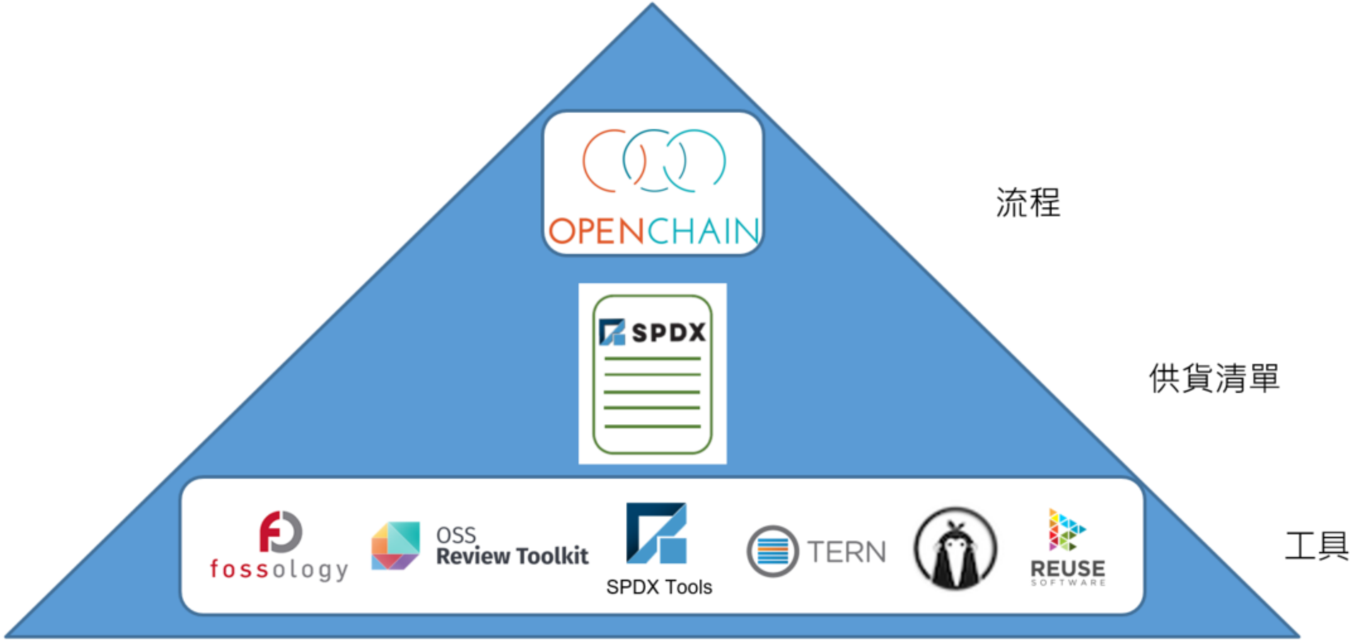
OpenChain 定義開源合規佈局



成果：可預測的 B2B 合規舉措



開源合規解決方案



https://compliance.linuxfoundation.org/

OpenChain 規範書

版本 2.0

在開源裡建立信任以構建軟體解決方案

https://github.com/OpenChain-Project/Specification-Translations/tree/master/zh-Hant/2.0

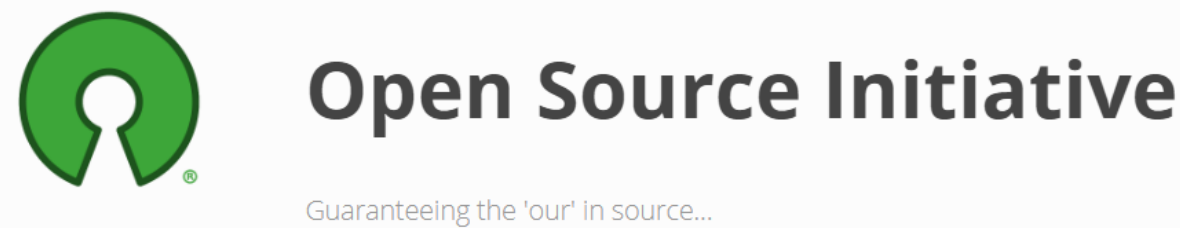
“開源軟體”

軟體程式依據一個或多個授權條款，該條款符合**開放原始碼促進會 (OpenSource.org)** 發布之開放原始碼定義 (Open Source Definition) 或**自由軟體基金會**發布之自由軟體定義 (Free Software Definition) 或類似條款。

The Open Source Definition

“Open source doesn't just mean access to the source code.”

“The distribution terms of open-source software must comply with the following criteria.”



Open Source Initiative [1]

Guaranteeing the 'our' in source...

img src: https://opensource.org/

1 Free Redistribution

2 Source Code

3 Derived Works

4 Integrity of The Author's Source Code

5 No Discrimination Against Persons or Groups

6 No Discrimination Against Fields of Endeavor

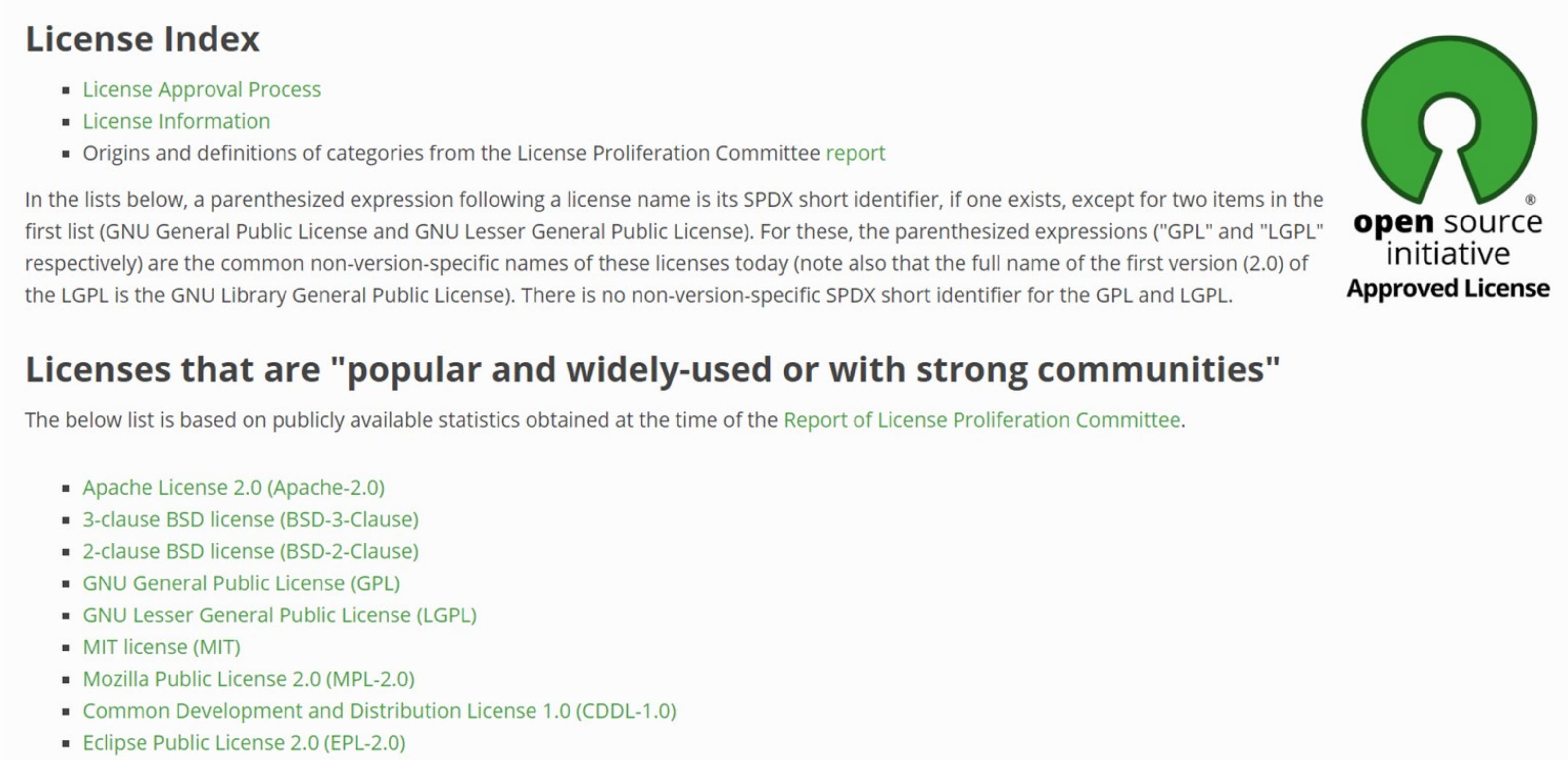
7 Distribution of License

8 License Must Not Be Specific to a Product

9 License Must Not Restrict Other Software

10 License Must Be Technology-Neutral

Open Source Licenses [2]



License Index

- License Approval Process
- License Information
- Origins and definitions of categories from the License Proliferation Committee report

In the lists below, a parenthesized expression following a license name is its SPDX short identifier, if one exists, except for two items in the first list (GNU General Public License and GNU Lesser General Public License). For these, the parenthesized expressions ("GPL" and "LGPL" respectively) are the common non-version-specific names of these licenses today (note also that the full name of the first version (2.0) of the LGPL is the GNU Library General Public License). There is no non-version-specific SPDX short identifier for the GPL and LGPL.

Licenses that are "popular and widely-used or with strong communities"

The below list is based on publicly available statistics obtained at the time of the Report of License Proliferation Committee.

- Apache License 2.0 (Apache-2.0)
- 3-clause BSD license (BSD-3-Clause)
- 2-clause BSD license (BSD-2-Clause)
- GNU General Public License (GPL)
- GNU Lesser General Public License (LGPL)
- MIT license (MIT)
- Mozilla Public License 2.0 (MPL-2.0)
- Common Development and Distribution License 1.0 (CDDL-1.0)
- Eclipse Public License 2.0 (EPL-2.0)

The Free Software Definition

The term "free" is used in the sense of "free speech," not of "free of charge."

FREE SOFTWARE FOUNDATION [3]

1 The freedom to run the program, for any purpose (freedom 0).

2 The freedom to study how the program works, and change it so it does your computing as you wish (freedom 1). Access to the source code is a precondition for this.

3 The freedom to redistribute copies so you can help your neighbor (freedom 2).

4 The freedom to distribute copies of your modified versions to others (freedom 3). By doing this you can give the whole community a chance to benefit from your changes. Access to the source code is a precondition for this.

Open Source and Free Software [4]

The term “open source” software is used by some people to mean more or less the same category as free software. ***It is not exactly the same class of software****: they accept some licenses that we consider too restrictive, and there are free software licenses they have not accepted. However, the differences in extension of the category are small: we know of only a few cases of source code that is open source but not free. In principle it could happen that some free programs are rejected as open source, but we don't know if that has ever happened.*

We prefer the term “free software” because it refers to freedom—something that the term “open source“ does not do.

OPENCHAIN
2.0

建立 OpenChain 流程的六大要點[5]

1、**方案**建立規範範圍、 開源**政策書**建立框架

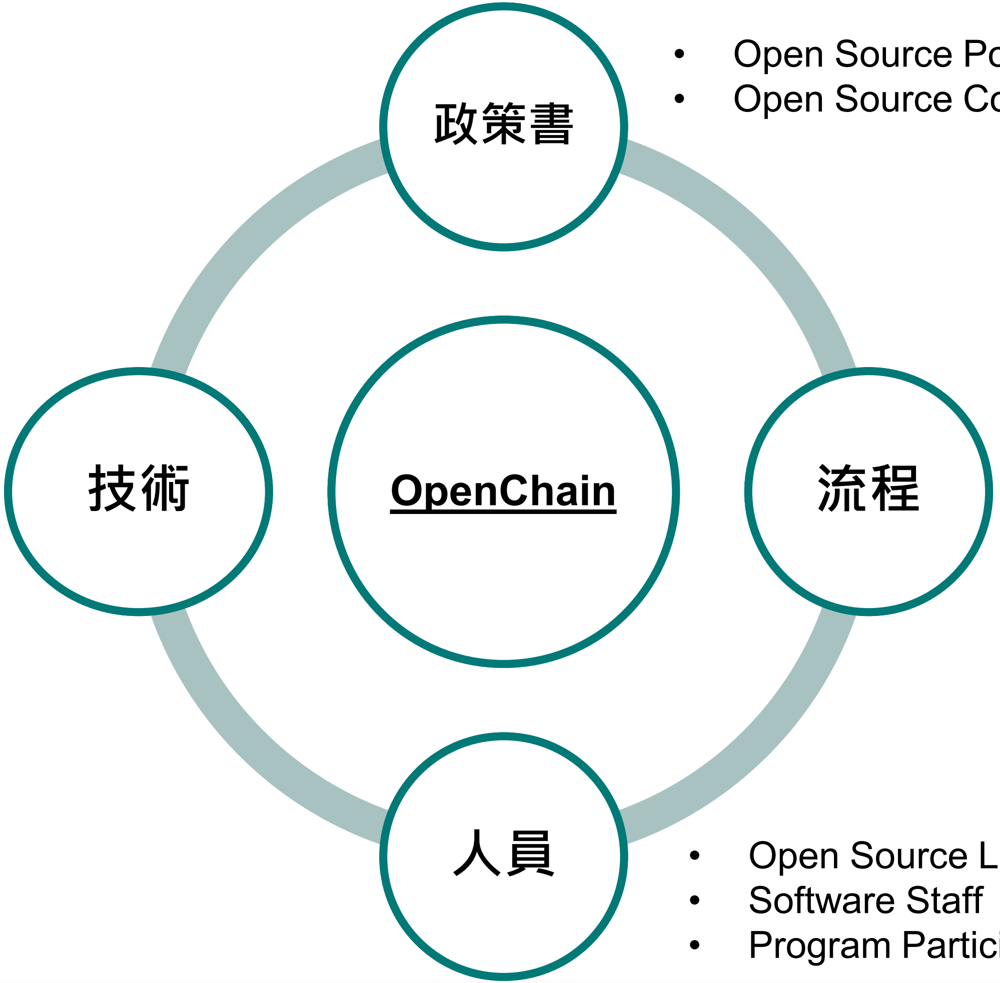
2、聯絡**窗口**、**資源配置**、**角色**及**責任**

3、開源軟體**清單的建立**流程

4、開源軟體**清單的驗證**、合規稽證產出流程

5、與開源**社群互動**規範

6、確認以上要點皆被**妥善記錄**、**保存**、以及**定期更新**



- Open Source Policy
- Open Source Contribution Policy

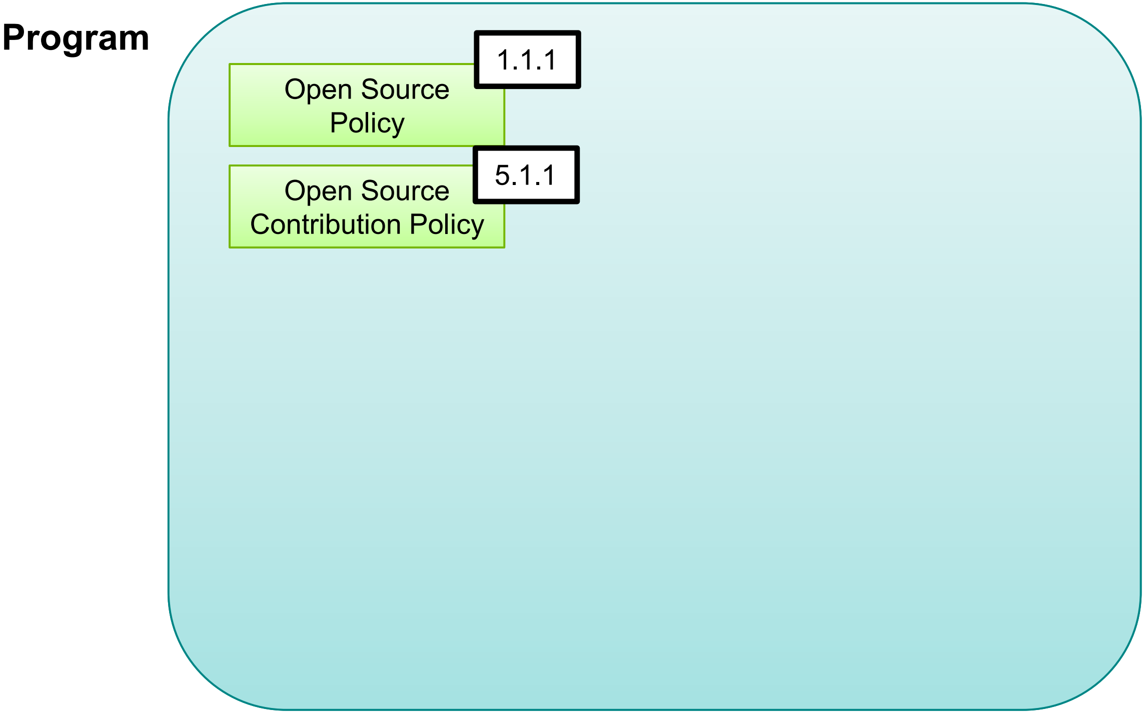
- Policy Implementation
- Program R&R and Implementation
- License Obligations
- Open Source Content Review and Approval
- Compliance Artifact Creation and Delivery
- Open Source License Compliance Inquiry
- Documentation
- Regularly updated

- License Scanning Tools
- Software BOM Management Tools
- SPDX Tools

- Open Source Liaison
- Software Staff
- Program Participants

Program

OpenChain 2.0 Specification



Program

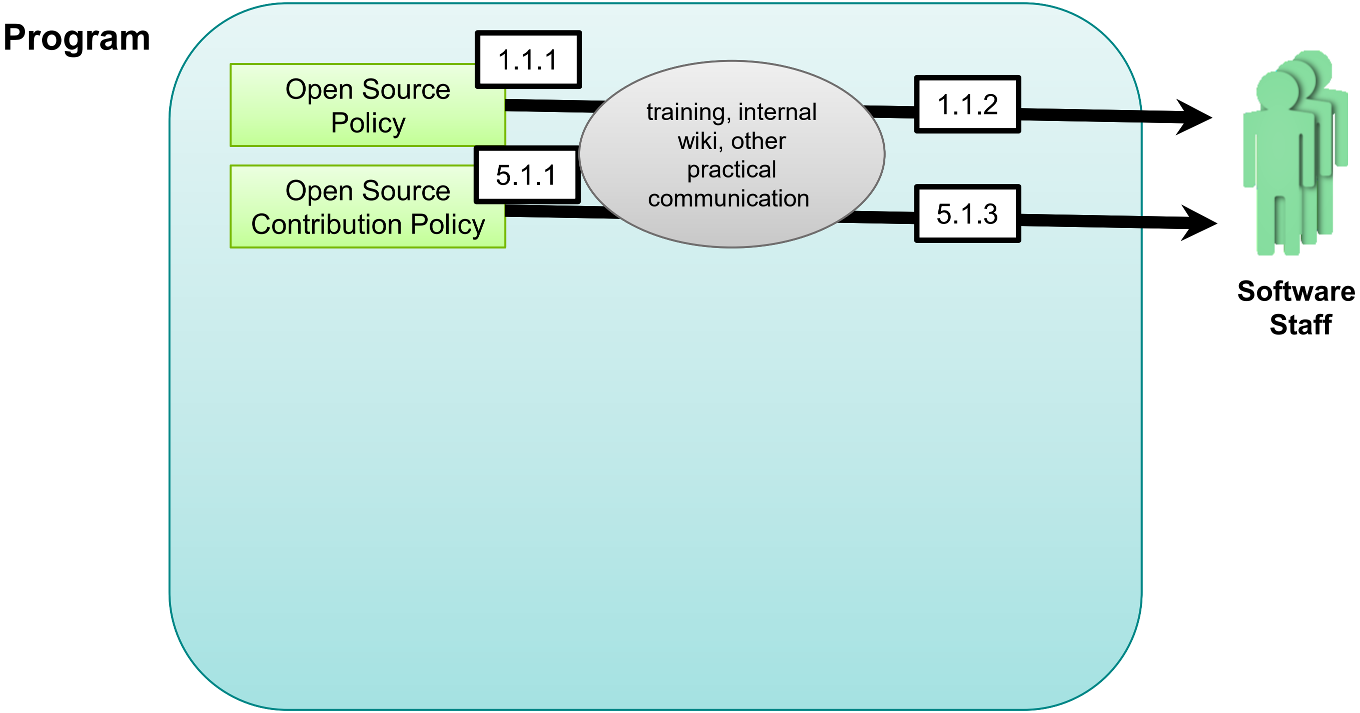
Open Source Policy

1.1.1

Open Source Contribution Policy

5.1.1

OpenChain 2.0 Specification



Program

Open Source Policy

1.1.1

Open Source Contribution Policy

5.1.1

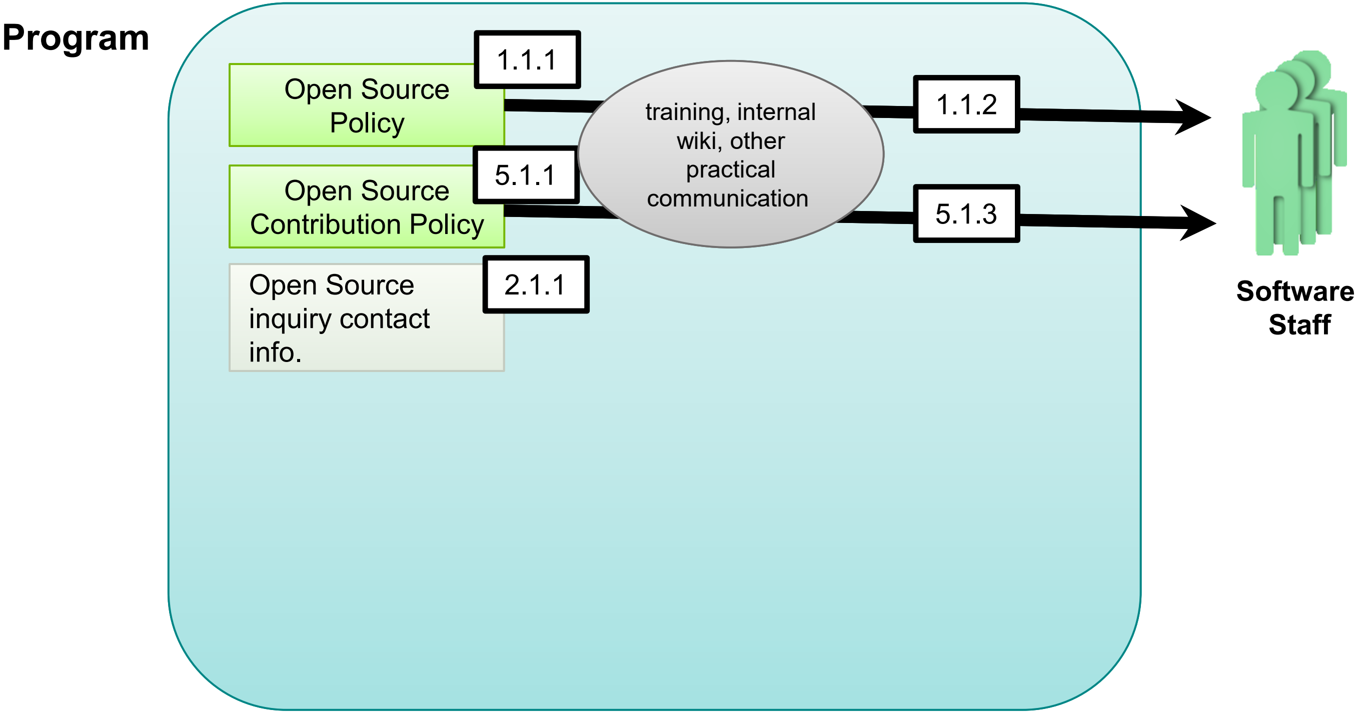
training, internal wiki, other practical communication

1.1.2

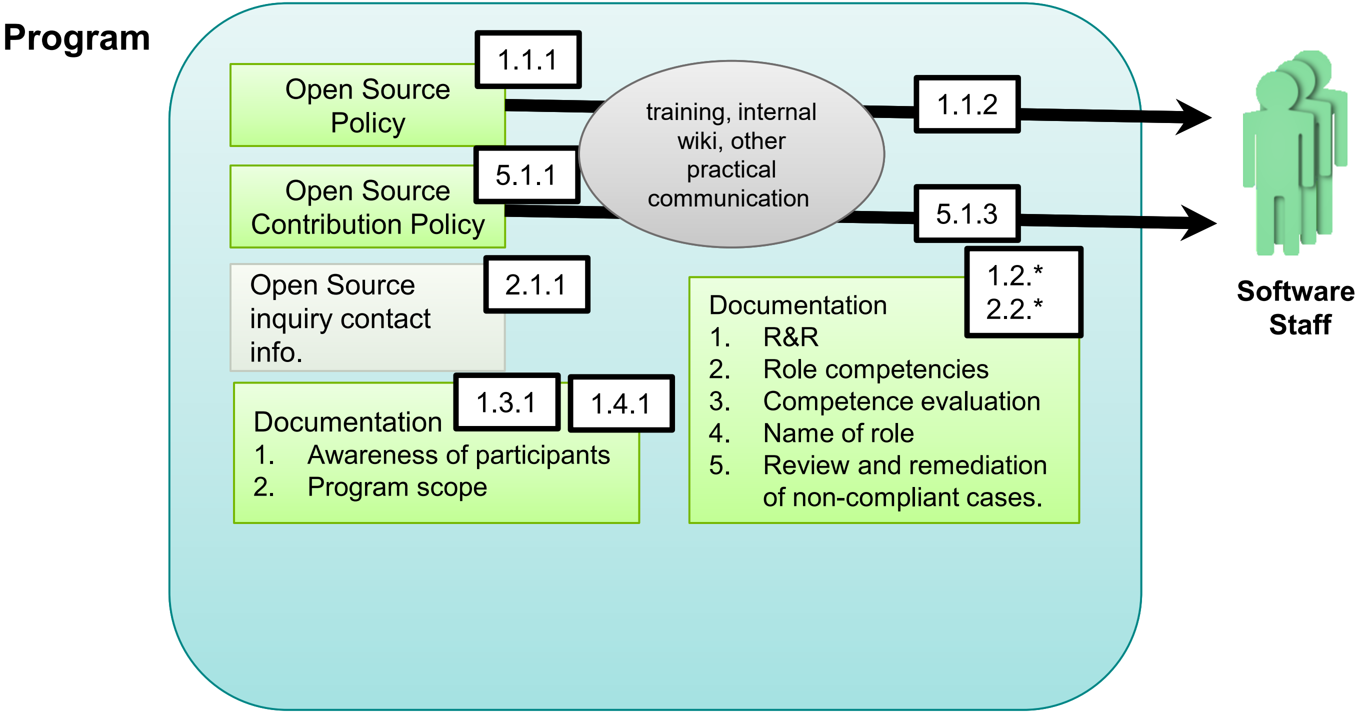
5.1.3

Software Staff

OpenChain 2.0 Specification


Program
Open Source Policy
1.1.1
Open Source Contribution Policy
5.1.1
Open Source inquiry contact info.
2.1.1
training, internal wiki, other practical communication
1.1.2
5.1.3
Software Staff

OpenChain 2.0 Specification



Program

Open Source Policy

1.1.1

Open Source Contribution Policy

5.1.1

training, internal wiki, other practical communication

1.1.2

5.1.3

Software Staff

Open Source inquiry contact info.

2.1.1

Documentation
1. R&R
2. Role competencies
3. Competence evaluation
4. Name of role
5. Review and remediation of non-compliant cases.

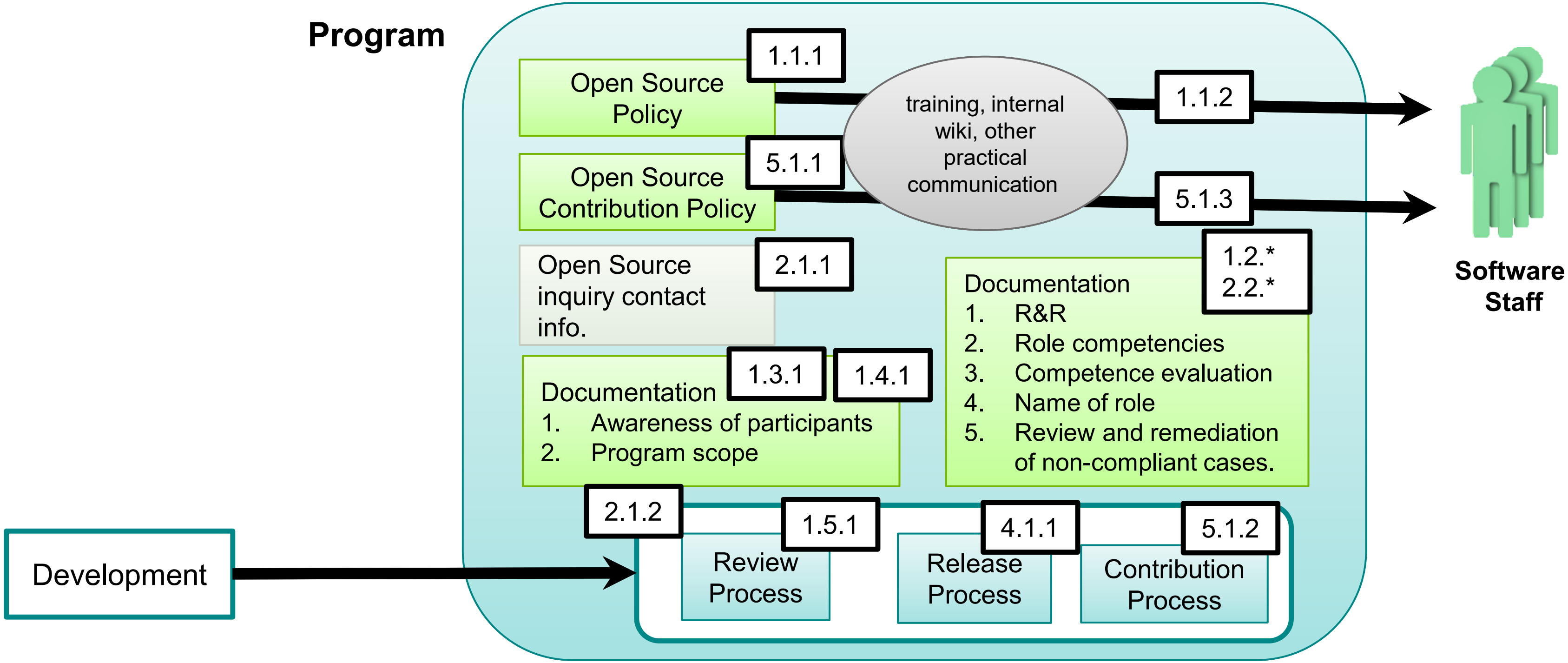
1.2.*
2.2.*

Documentation
1. Awareness of participants
2. Program scope

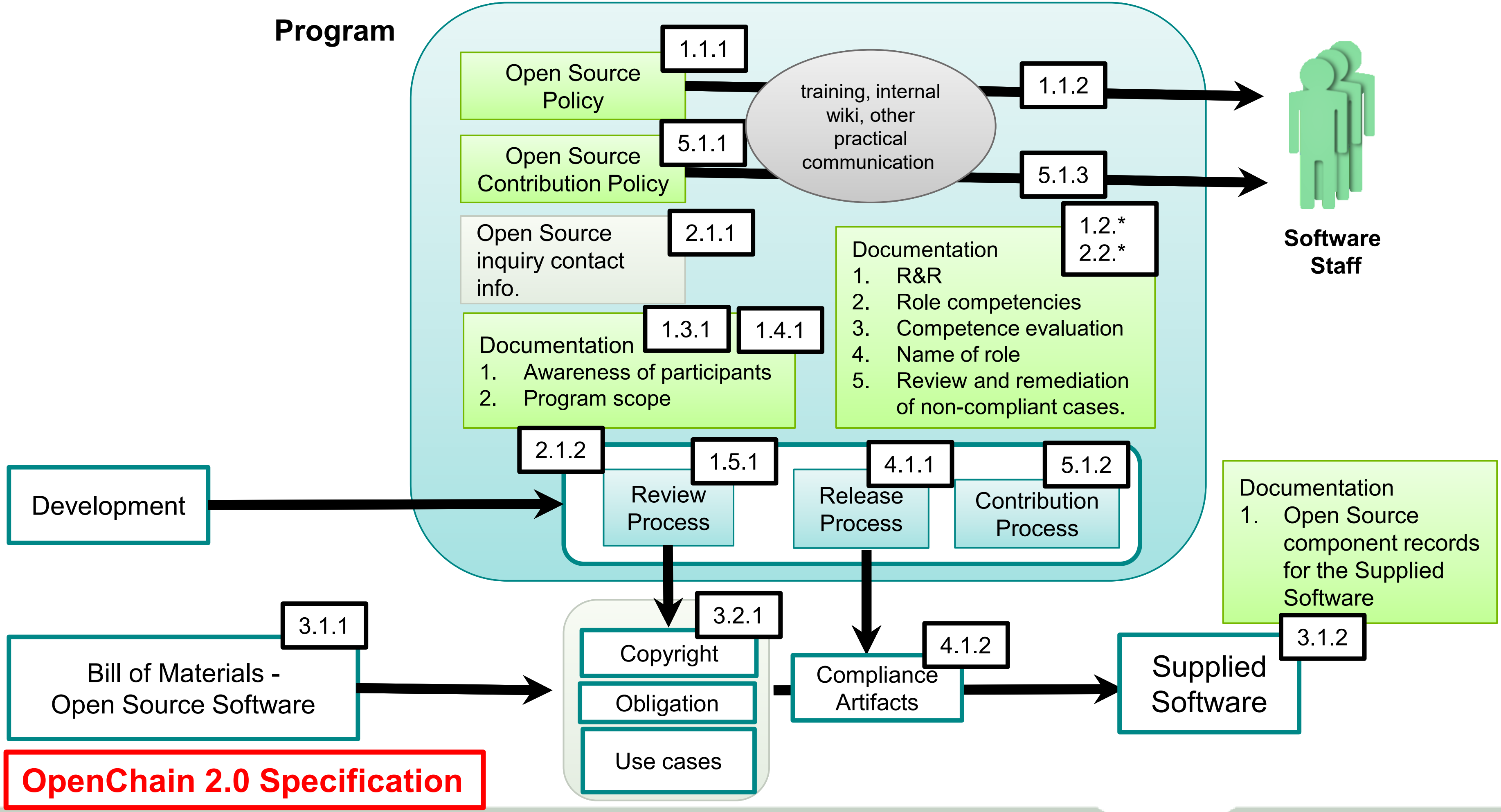
1.3.1

1.4.1

OpenChain 2.0 Specification



OpenChain 2.0 Specification



Program

Open Source Policy 1.1.1

Open Source Contribution Policy 5.1.1

training, internal wiki, other practical communication

1.1.2

5.1.3

Software Staff

Open Source inquiry contact info. 2.1.1

Documentation 1.3.1 1.4.1
1. Awareness of participants
2. Program scope

Documentation 1.2.* 2.2.*
1. R&R
2. Role competencies
3. Competence evaluation
4. Name of role
5. Review and remediation of non-compliant cases.

Development

2.1.2

Review Process 1.5.1

Release Process 4.1.1

Contribution Process 5.1.2

Documentation
1. Open Source component records for the Supplied Software

Bill of Materials - Open Source Software 3.1.1

Copyright 3.2.1

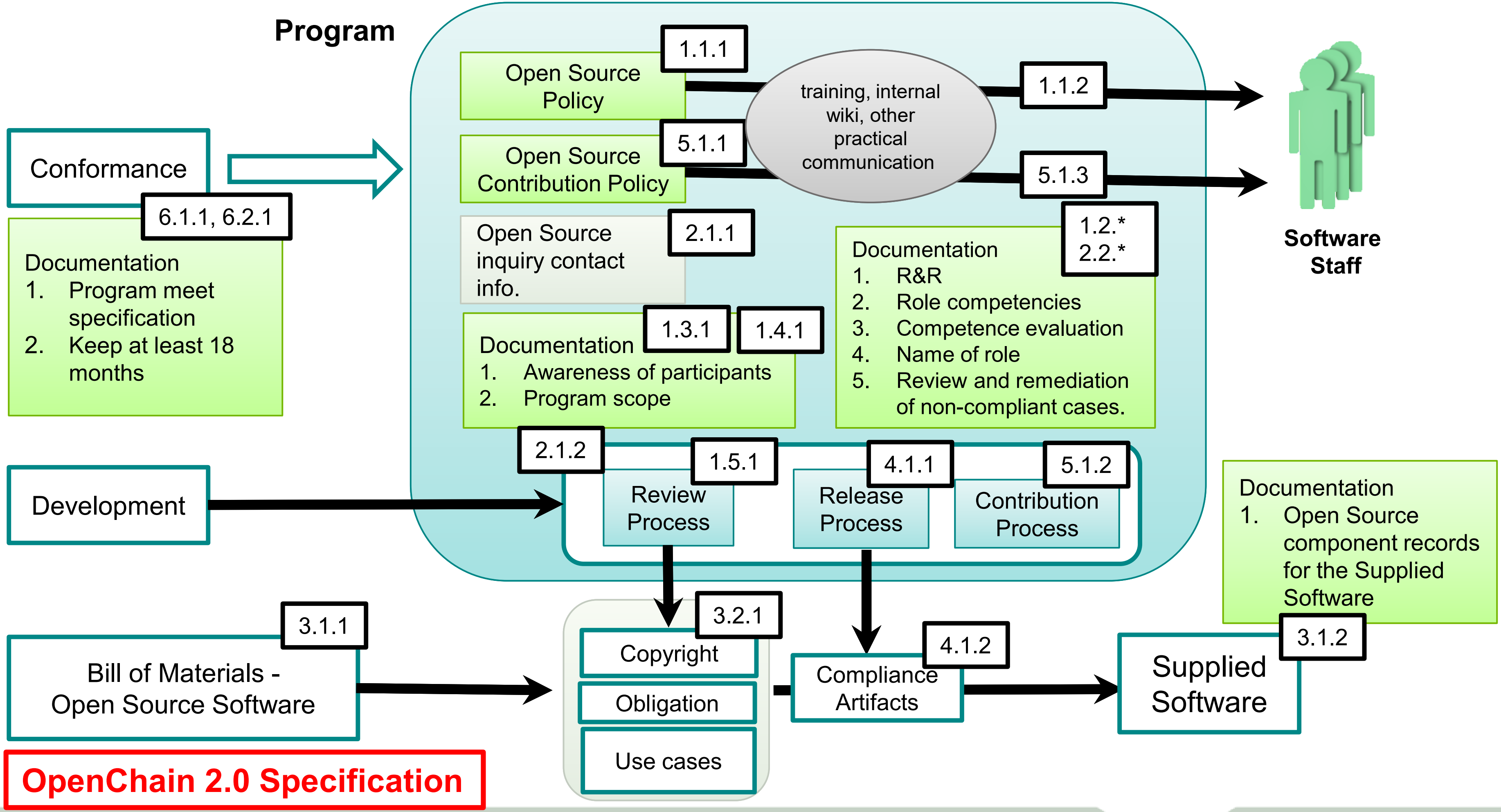
Obligation

Use cases

Compliance Artifacts 4.1.2

Supplied Software 3.1.2

OpenChain 2.0 Specification



Program

Open Source Policy 1.1.1

Open Source Contribution Policy 5.1.1

training, internal wiki, other practical communication

1.1.2

5.1.3

Software Staff

Conformance

6.1.1, 6.2.1

Documentation
1. Program meet specification
2. Keep at least 18 months

Open Source inquiry contact info. 2.1.1

Documentation 1.3.1 1.4.1
1. Awareness of participants
2. Program scope

Documentation 1.2.* 2.2.*
1. R&R
2. Role competencies
3. Competence evaluation
4. Name of role
5. Review and remediation of non-compliant cases.

Development

2.1.2

Review Process 1.5.1

Release Process 4.1.1

Contribution Process 5.1.2

Documentation
1. Open Source component records for the Supplied Software

3.1.1

Bill of Materials - Open Source Software

3.2.1

Copyright

Obligation

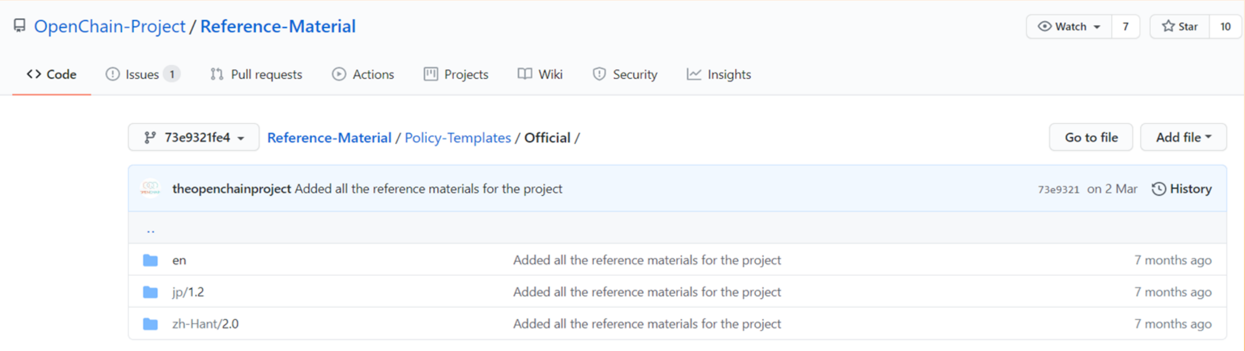
Use cases

Compliance Artifacts 4.1.2

Supplied Software 3.1.2

OpenChain 2.0 Specification

Open Source Policy Template



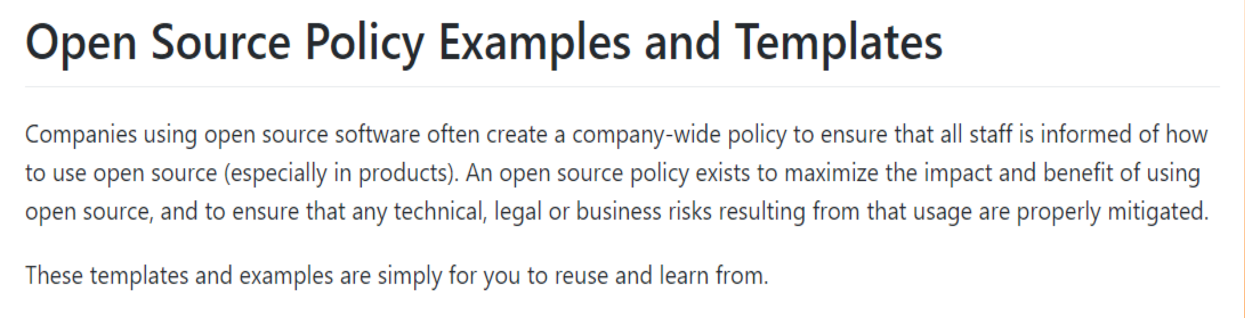
OpenChain-Project / **Reference-Material**

Reference-Material / Policy-Templates / **Official** /

theopenchainproject Added all the reference materials for the project — 73e9321 on 2 Mar

..

en	Added all the reference materials for the project	7 months ago
jp/1.2	Added all the reference materials for the project	7 months ago
zh-Hant/2.0	Added all the reference materials for the project	7 months ago

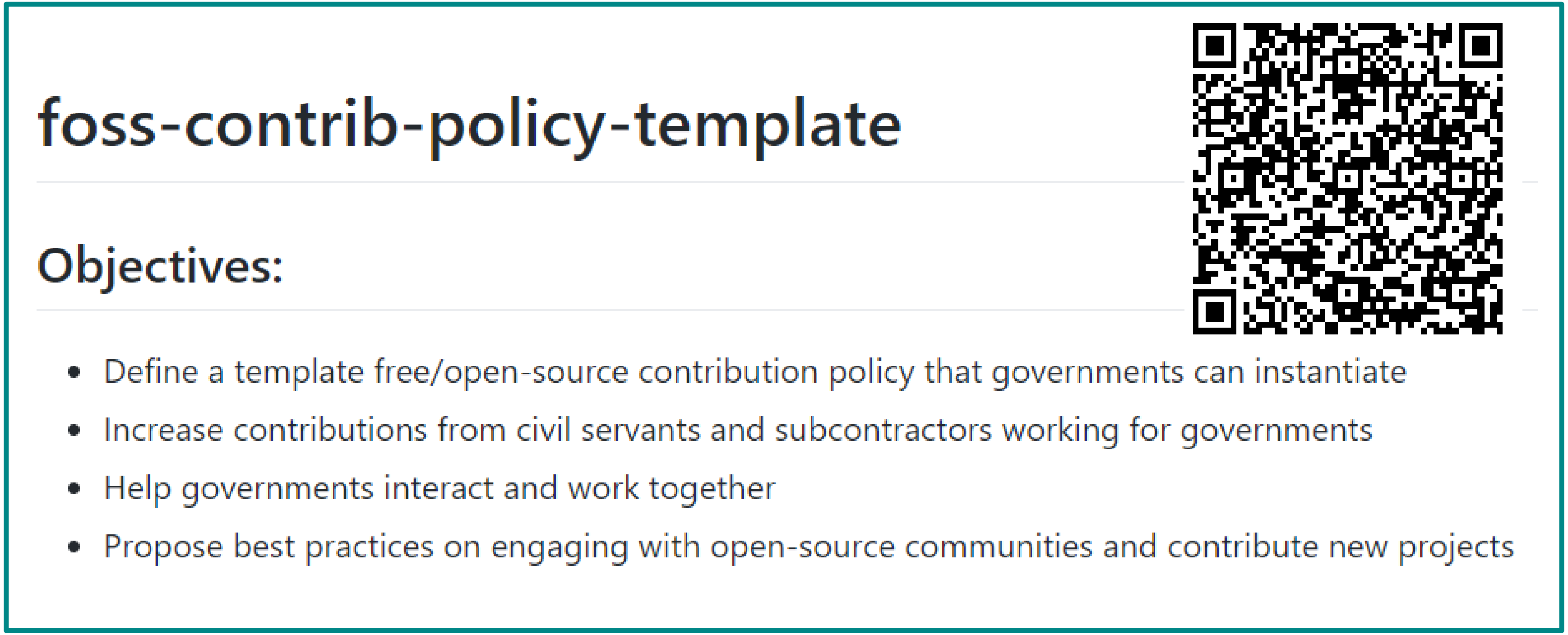


Open Source Policy Examples and Templates

Companies using open source software often create a company-wide policy to ensure that all staff is informed of how to use open source (especially in products). An open source policy exists to maximize the impact and benefit of using open source, and to ensure that any technical, legal or business risks resulting from that usage are properly mitigated.

These templates and examples are simply for you to reuse and learn from.

Open Source Contribution Policy

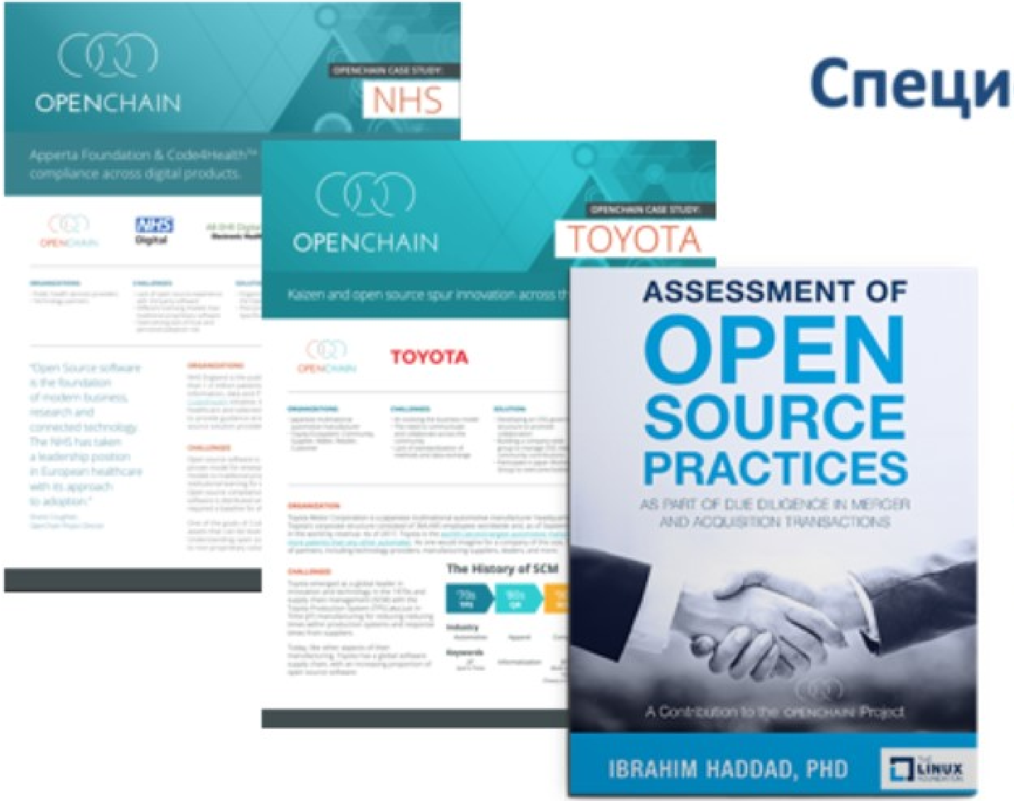


foss-contrib-policy-template

Objectives:

- Define a template free/open-source contribution policy that governments can instantiate
- Increase contributions from civil servants and subcontractors working for governments
- Help governments interact and work together
- Propose best practices on engaging with open-source communities and contribute new projects

廣泛的参照素材



OPENCHAIN

OPENCHAIN CASE STUDY:

NHS

Apperta Foundation & Code4Health™ compliance across digital products.

OPENCHAIN

OPENCHAIN CASE STUDY:

TOYOTA

Kaizen and open source spur innovation across th

ASSESSMENT OF OPEN SOURCE PRACTICES

AS PART OF DUE DILIGENCE IN MERGER AND ACQUISITION TRANSACTIONS

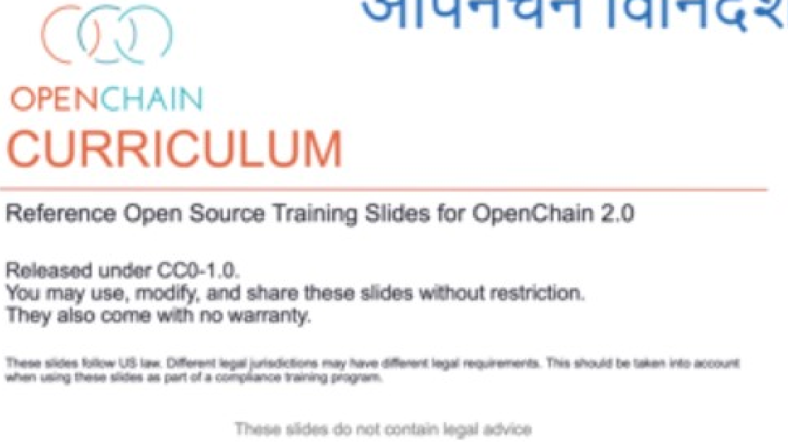
A Contribution to the OPENCHAIN Project

IBRAHIM HADDAD, PHD

Спецификация OpenChain

Версия 1.2

ओपनचेन विनिर्देश



OPENCHAIN

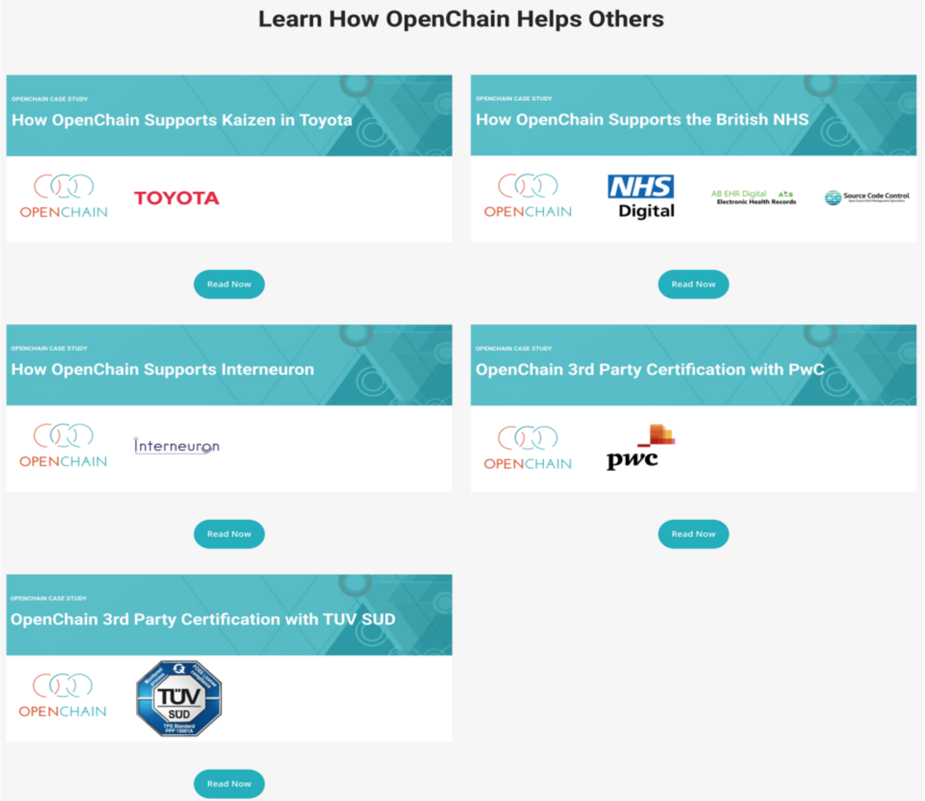
CURRICULUM

Reference Open Source Training Slides for OpenChain 2.0

Released under CC0-1.0.
You may use, modify, and share these slides without restriction.
They also come with no warranty.

These slides follow US law. Different legal jurisdictions may have different legal requirements. This should be taken into account when using these slides as part of a compliance training program.

These slides do not contain legal advice



Learn How OpenChain Helps Others

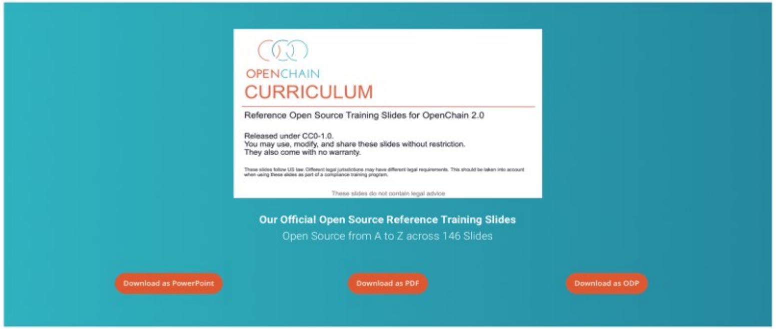
OPENCHAIN CASE STUDY
How OpenChain Supports Kaizen in Toyota

OPENCHAIN CASE STUDY
How OpenChain Supports the British NHS

OPENCHAIN CASE STUDY
How OpenChain Supports Interneuron

OPENCHAIN CASE STUDY
OpenChain 3rd Party Certification with PwC

OPENCHAIN CASE STUDY
OpenChain 3rd Party Certification with TUV SUD



OPENCHAIN
CURRICULUM

Reference Open Source Training Slides for OpenChain 2.0

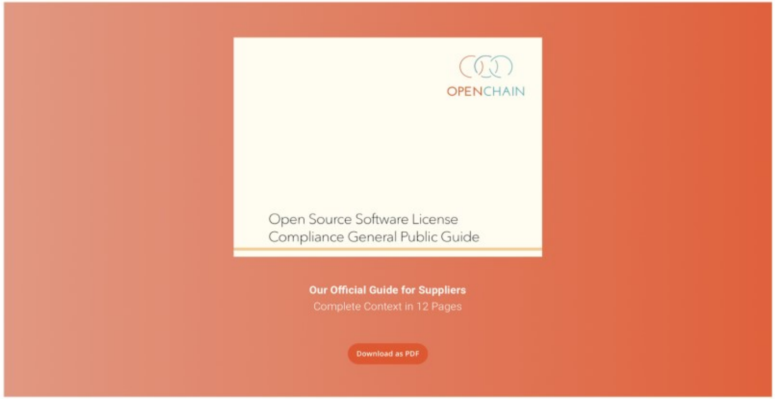
Released under CC0-1.0.
You may use, modify, and share these slides without restriction.
They also come with no warranty.

These slides follow US law. Different legal jurisdictions may have different legal requirements. This should be taken into account when using these slides as part of a compliance training program.

These slides do not contain legal advice

Our Official Open Source Reference Training Slides

Open Source from A to Z across 146 Slides

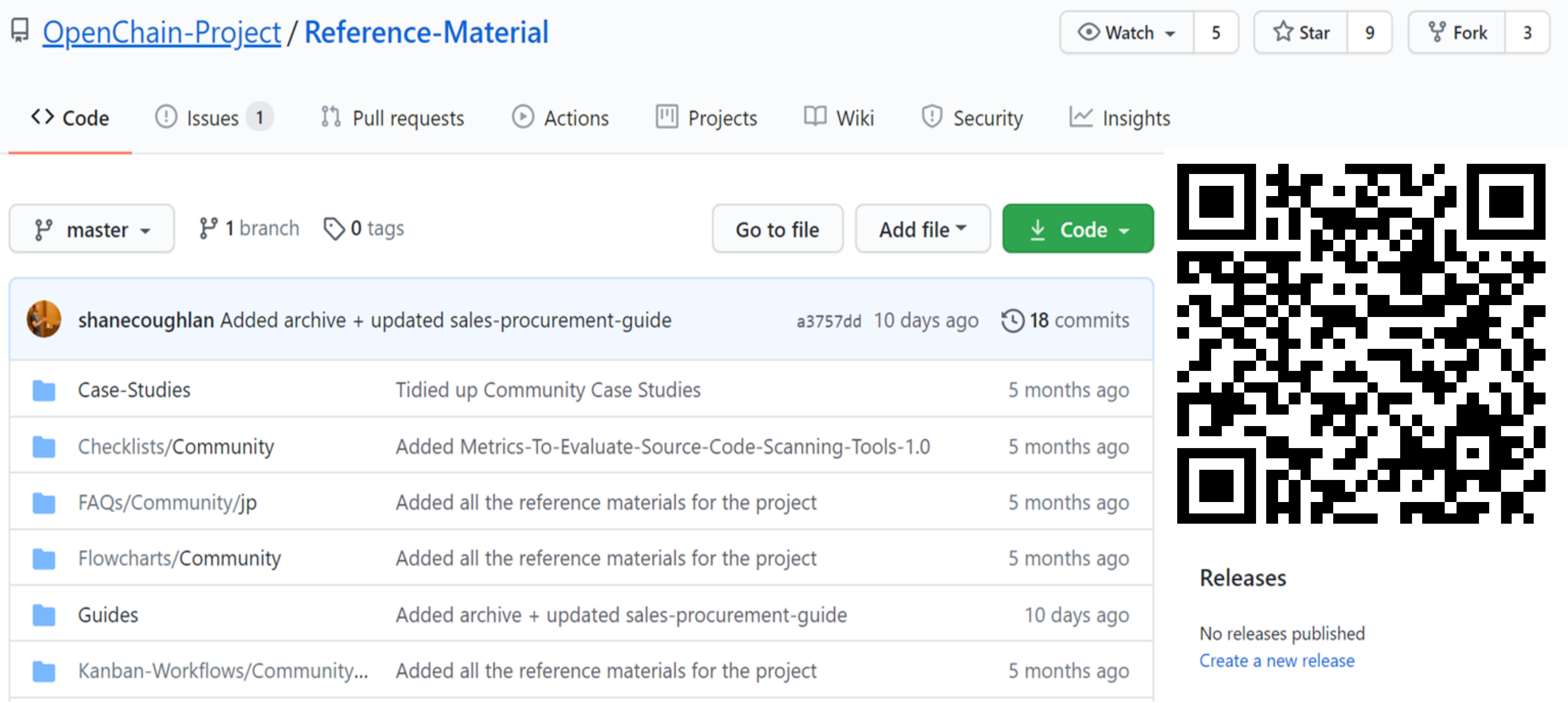


OPENCHAIN

Open Source Software License Compliance General Public Guide

Our Official Guide for Suppliers

Complete Context in 12 Pages



OpenChain-Project / Reference-Material

shanecoughlan Added archive + updated sales-procurement-guide a3757dd 10 days ago 18 commits

Case-Studies	Tidied up Community Case Studies	5 months ago
Checklists/Community	Added Metrics-To-Evaluate-Source-Code-Scanning-Tools-1.0	5 months ago
FAQs/Community/jp	Added all the reference materials for the project	5 months ago
Flowcharts/Community	Added all the reference materials for the project	5 months ago
Guides	Added archive + updated sales-procurement-guide	10 days ago
Kanban-Workflows/Community...	Added all the reference materials for the project	5 months ago

Releases

No releases published
Create a new release

SPDX [6]

Trust for software packages

Software Package Data Exchange (SPDX) is a file format used to document information on the software licenses under which a given piece of computer software is distributed.

FOSSology [7]

Free scanning technology

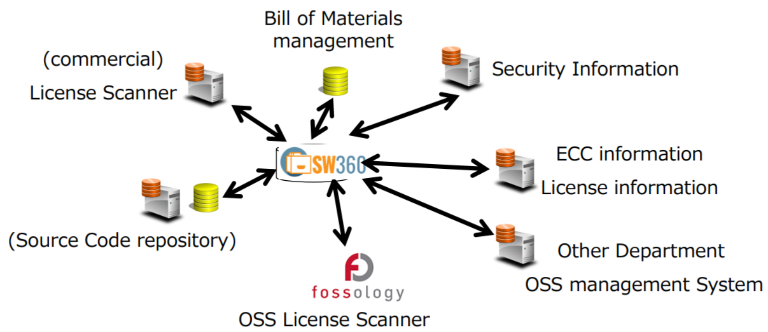
FOSSology is a open source license compliance software system and toolkit

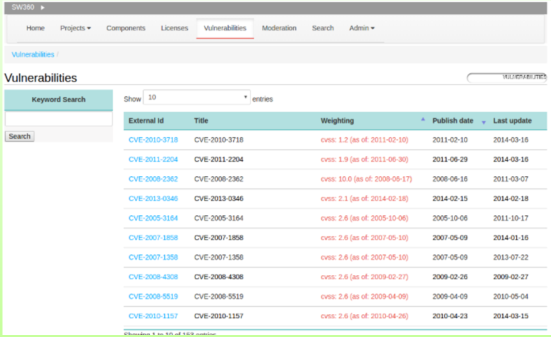
Eclipse SW360 [8]

Software catalogue application

SW360 aims to provide the central place in the organization to share the information of software components

SW360





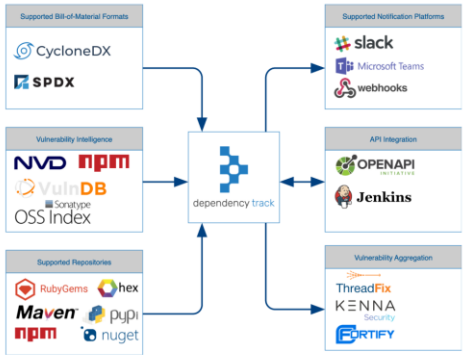
Vulnerabilities

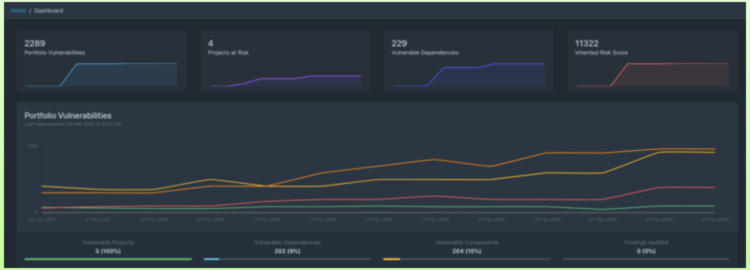
Show 10 entries

External Id	Title	Weighting	Publish date	Last update
CVE-2010-3718	CVE-2010-3718	cvss: 1.2 (as of: 2011-02-10)	2011-02-10	2014-03-16
CVE-2011-2204	CVE-2011-2204	cvss: 1.9 (as of: 2011-06-30)	2011-06-29	2014-03-16
CVE-2008-2362	CVE-2008-2362	cvss: 10.0 (as of: 2008-06-17)	2008-06-16	2011-03-07
CVE-2013-0346	CVE-2013-0346	cvss: 2.1 (as of: 2014-02-18)	2014-02-15	2014-02-18
CVE-2005-3164	CVE-2005-3164	cvss: 2.6 (as of: 2005-10-06)	2005-10-06	2011-10-17
CVE-2007-1858	CVE-2007-1858	cvss: 2.6 (as of: 2007-05-10)	2007-05-09	2014-01-16
CVE-2007-1358	CVE-2007-1358	cvss: 2.6 (as of: 2007-05-10)	2007-05-09	2013-07-22
CVE-2008-4308	CVE-2008-4308	cvss: 2.6 (as of: 2009-02-27)	2009-02-26	2009-02-27
CVE-2008-5519	CVE-2008-5519	cvss: 2.6 (as of: 2009-04-09)	2009-04-09	2010-05-04
CVE-2010-1157	CVE-2010-1157	cvss: 2.6 (as of: 2010-04-26)	2010-04-23	2014-03-15

Showing 1 to 10 of 153 entries

Dependency-Track [9]





A Simple Logo, A Significant Meaning

OPENCHAIN
1.0

OPENCHAIN
1.1

OPENCHAIN
1.2

OPENCHAIN
2.0

Quality Open Source Compliance Defined

對供應商及客戶都具自由度的評鑑選擇

OpenChain 評核可透過下列途徑達成：

1. 線上自我測驗

2. 獨立合規評估

3. 公正第三方驗證

Self-Certification / 線上自我測驗

Self-Certification is the OpenChain standard approach. The organization assesses its Open Source Program and OpenChain deems the program as OpenChain Conformant

https://certification.openchainproject.org

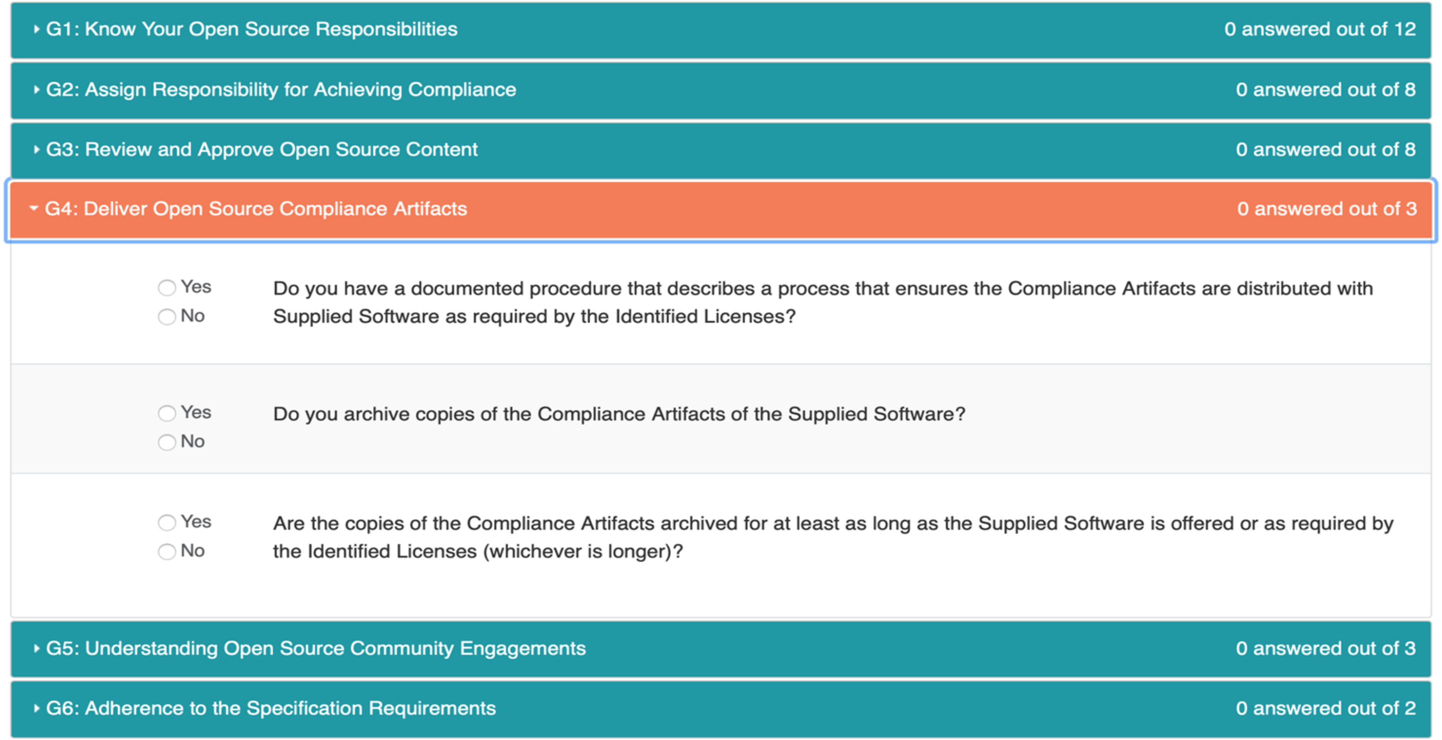
Independent Compliance Assessment/ 獨立合規評估

An independent party such as a law firm, consultancy or accounting firm reviews the product of an OpenChain Self-Assessment and offers guidance on whether they perceive it as complete. Despite all opportunities of adding value, the organization remains responsible for the Self-Certification.

https://certification.openchainproject.org

OPENCHAIN

線上自評問卷



▸ G1: Know Your Open Source Responsibilities — 0 answered out of 12

▸ G2: Assign Responsibility for Achieving Compliance — 0 answered out of 8

▸ G3: Review and Approve Open Source Content — 0 answered out of 8

▾ G4: Deliver Open Source Compliance Artifacts — 0 answered out of 3

○ Yes ○ 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?
○ Yes ○ No	Do you archive copies of the Compliance Artifacts of the Supplied Software?
○ Yes ○ 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: Understanding Open Source Community Engagements — 0 answered out of 3

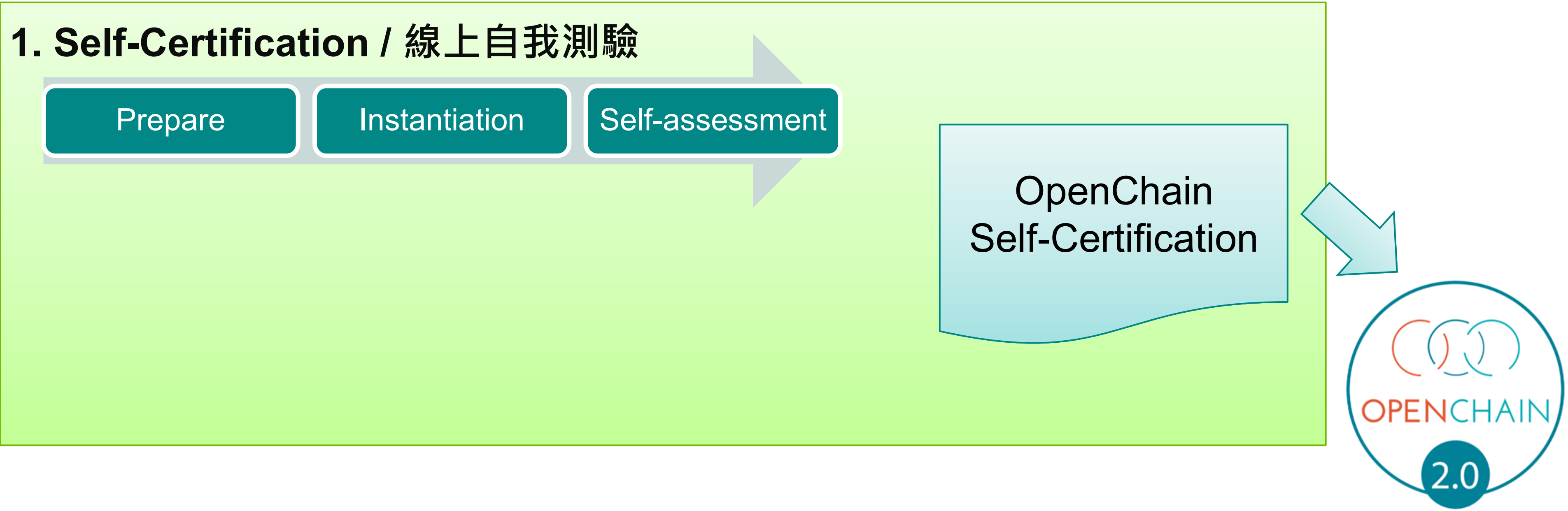
▸ G6: Adherence to the Specification Requirements — 0 answered out of 2

Third-Party Certification / 公正第三方驗證

Third-Party Certification is a process whereby a certification authority guides a company through an OpenChain Conformance Process. The certification authority then issues a formal certification document. This activity maps precisely to the forms of third-party certification observed around automotive, infrastructure and similar fields.

OpenChain 評核流程

Organization



1. **Self-Certification / 線上自我測驗**

Prepare

Instantiation

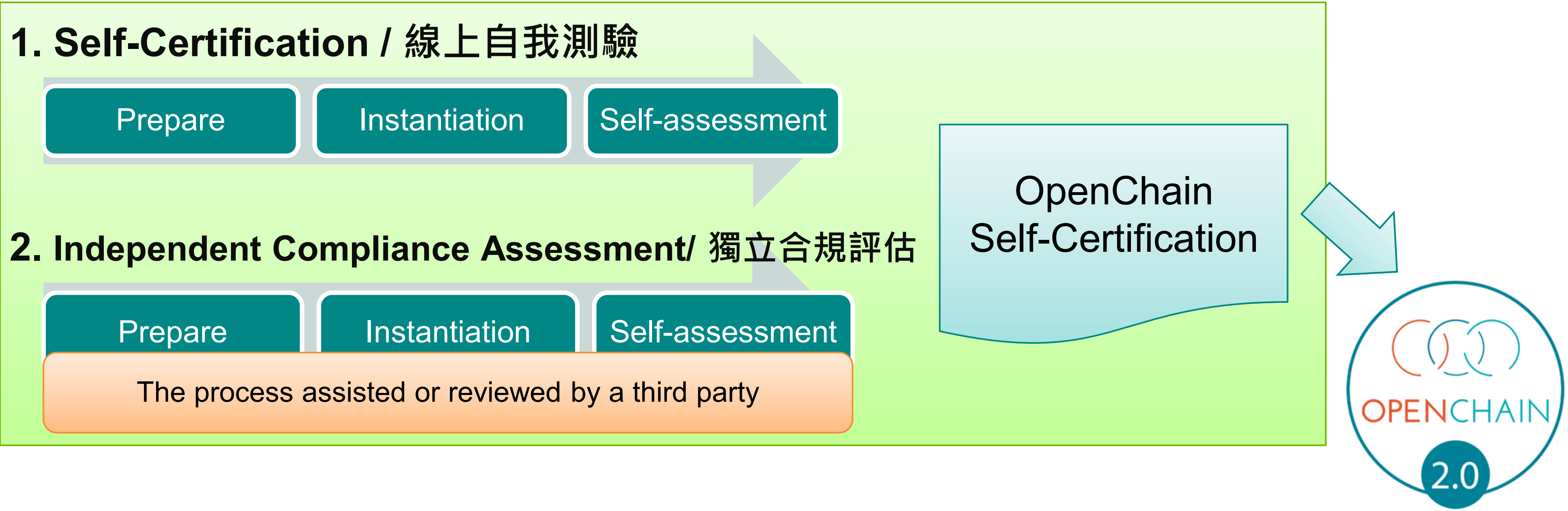
Self-assessment

OpenChain Self-Certification

OpenChain 評核流程

Organization

Third-party



1. Self-Certification / 線上自我測驗

Prepare

Instantiation

Self-assessment

2. Independent Compliance Assessment/ 獨立合規評估

Prepare

Instantiation

Self-assessment

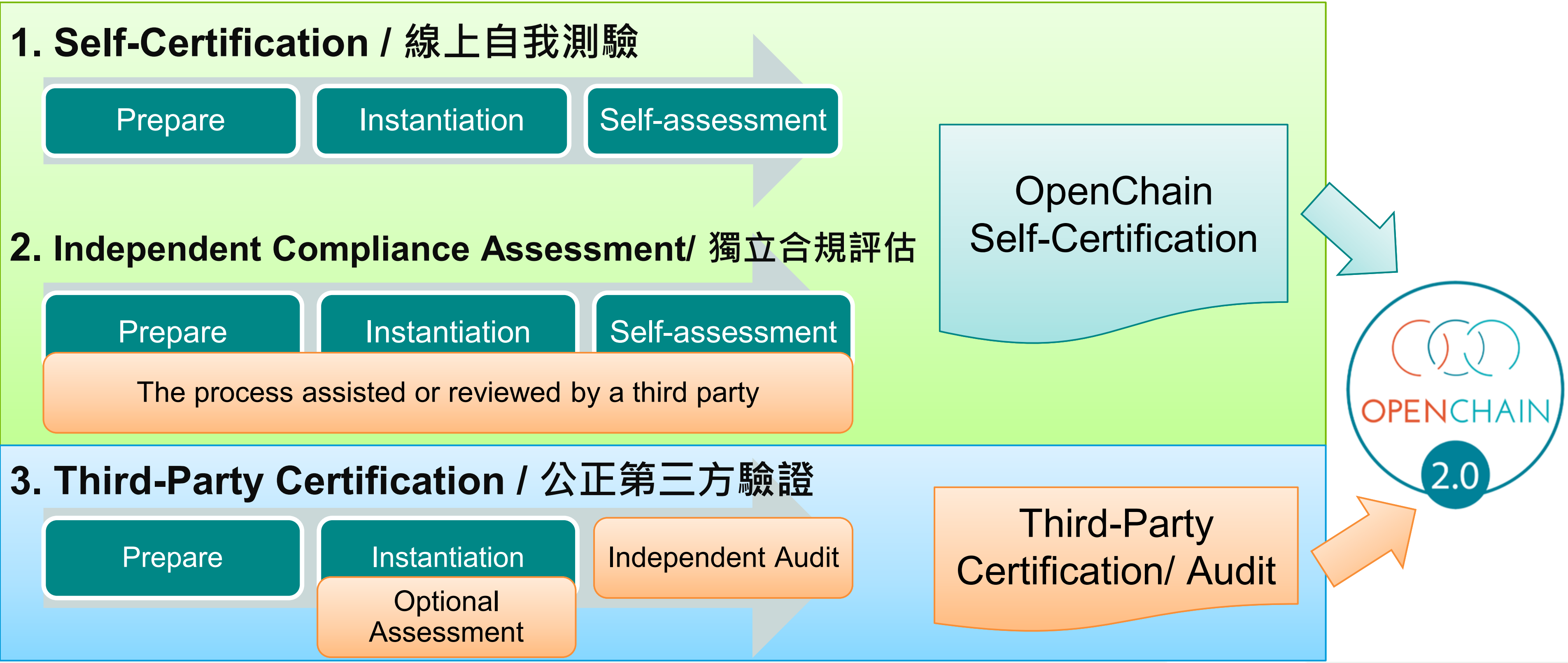
The process assisted or reviewed by a third party

OpenChain Self-Certification

OpenChain 評核流程

Organization

Third-party



1. Self-Certification / 線上自我測驗

Prepare

Instantiation

Self-assessment

2. Independent Compliance Assessment/ 獨立合規評估

Prepare

Instantiation

Self-assessment

The process assisted or reviewed by a third party

OpenChain Self-Certification

3. Third-Party Certification / 公正第三方驗證

Prepare

Instantiation

Optional Assessment

Independent Audit

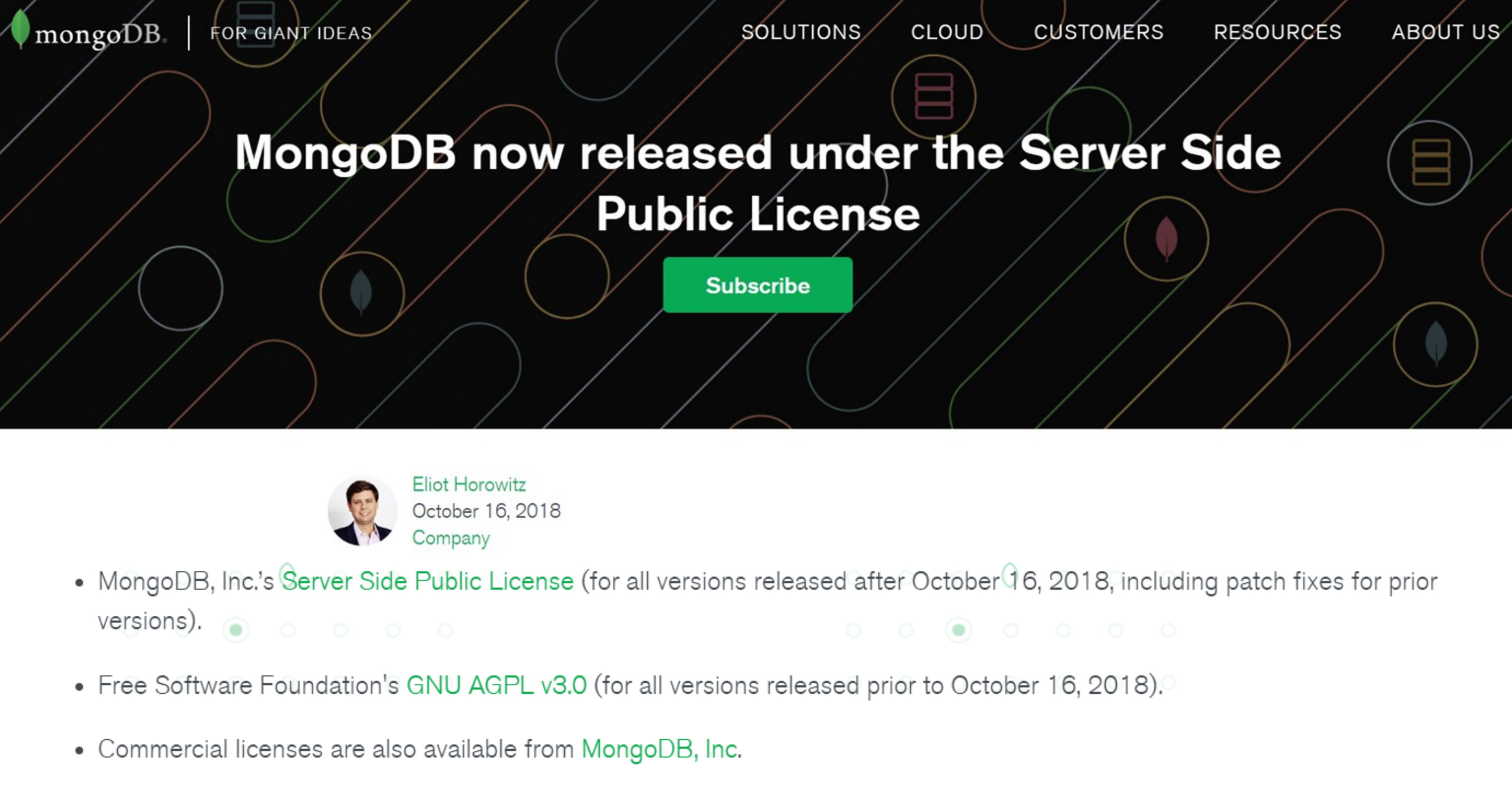
Third-Party Certification/ Audit

拿到 OpenChain 認證後
組織內所有產品皆需遵循此流程?

OpenChain 是否能 消弭所有使用開源軟體之風險?

開源軟體清單的驗證、合規稽證
產出只需做一次

往後不會有合規議題?



MongoDB now released under the Server Side Public License

Eliot Horowitz
October 16, 2018
Company

- MongoDB, Inc.'s Server Side Public License (for all versions released after October 16, 2018, including patch fixes for prior versions).
- Free Software Foundation's GNU AGPL v3.0 (for all versions released prior to October 16, 2018).
- Commercial licenses are also available from MongoDB, Inc.

成為 OpenChain 其中一員

加入 OpenChain 社群：

https://www.openchainproject.org/get-started

OpenChain 臺灣網站:

https://openchain-project.github.io/OpenChain-TWG/

Telegram 討論頻道

https://t.me/joinchat/O6BDhVXYm17Bm8_4s-aZlg

訂閱臺灣 OpenChain 官方社群 Mailing List

https://lists.openchainproject.org/g/taiwan-wg

Telegram channel

Mailing list

OpenChain Project Taiwan Work Group

SZ Lin （ 林上智 ）<sz.lin@moxa.com>
Lucien C.H. Lin （ 林誠夏 ）<lucien@ocf.tw>

Thank You

MOXA®

Reliable Networks ▲ Sincere Service

References

[1] https://opensource.org/osd-annotated

[2] https://opensource.org/licenses/category

[3] https://www.fsf.org/

[4] https://www.gnu.org/philosophy/categories.html.en

[5] https://www.slideshare.net/szlin/openchain-the-industry-standard-for-open-source-compliance-237890869

[6] https://spdx.dev/

[7] https://www.fossology.org/

[8] https://www.eclipse.org/sw360/

[9] https://dependencytrack.org/

References

[10] https://docs.google.com/presentation/d/1E1am2wo0K3PbovtoByEOkvLWK2SLfv_cLFXo7VXJJ9o/edit#slide=id.g63a2ddb8b6_7_78