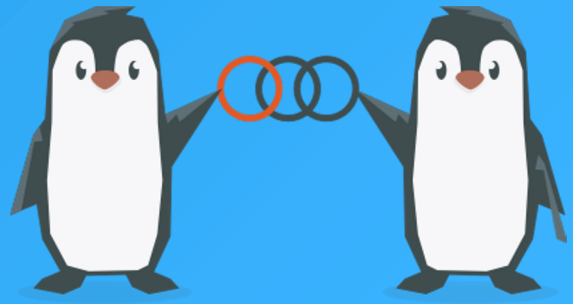
The OpenChain Project

Japan Work Group Meeting #31
2024-06-27

THE LINUX FOUNDATION

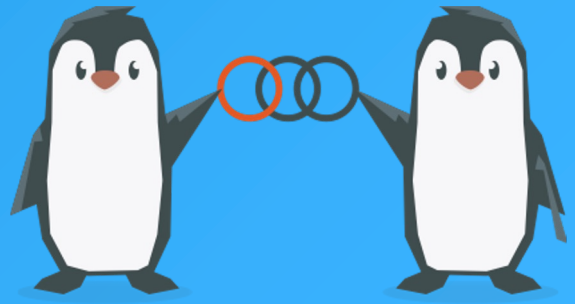
OPENCHAIN



Key Project News

THE LINUX FOUNDATION

OPENCHAIN



Public Comment Period

Proposed Draft Updates to ISO/IEC 5230 and ISO/IEC 18974

Starting 2024-06-19 ~ Ending 2024-012-19

- The OpenChain Project has announced the beginning of its six month Public Comment Period for proposed draft updates to the open source license compliance (ISO/IEC 5230:2020) and open source security assurance (ISO/IEC 18974:2023) specifications.
- As per our specification development process outlined in the project FAQ, this Public Comment Period will run for six months, and it will be followed by a three month Freeze Period.

THE LINUX FOUNDATION OPENCHAIN

Review of suggested changes to ISO/IEC 5230:2020

- Current ISO standard:
  - https://github.com/OpenChain-Project/License-Compliance-Specification/blob/master/ISO-5230-2020/en/ISO-5230-2020.md
- Current Next Generation Draft (pre-public comments period):
  - https://github.com/OpenChain-Project/License-Compliance-Specification/blob/master/3.0/en/openchain-license-compliance-3.0.md
- All open issues have been closed by the Specification Work Group
  - https://github.com/OpenChain-Project/License-Compliance-Specification/issues?q=is%3Aissue+is%3Aclosed

Next:

- Six month public comment period launched 19th June 2024 as per our specification development process:
  - https://openchainproject.org/resources/faq#specification-development-questions
- This will be followed by a Three Month freeze period

Example Suggestion for ISO/IEC 5230:2020

```
### 3 - Requirements

- 3.1 - Program foundation
- - 3.1.1 - Policy
- - 3.1.2 - Competence
- - 3.1.3 - Awareness
- - 3.1.4 - Program scope
- - 3.1.5 - License obligations

- 3.2 - Relevant tasks defined and supported
- - 3.2.1 - Access
- - 3.2.2 - Effectively

- 3.3 - Open source content review and approval
- - 3.3.1 - Bill of materials
- - 3.3.2 - License compliance

- 3.4 - Compliance artifact creation and delivery
- - 3.4.1 - Compliance artifacts

- 3.5 - Understanding open source community engagements
- - 3.5.1 - Contributions

- 3.6 - Adherence to the specification requirements
- - 3.6.1 - Conformance
- - 3.6.2 - Duration
```

```
### 3 - Requirements

- 3.1 - Program foundation
- - 3.1.4 - Program scope
- - 3.1.1 - Policy
- - 3.1.3 - Awareness

- 3.2 - Relevant tasks defined and supported
- - 3.2.1 - Access
- - 3.2.2 - Competence
- - 3.2.3 - Effectively

- 3.3 - Open source content review and approval
- - 3.3.1 - Bill of materials
- - 3.3.2 - License obligations
- - 3.3.3 - License compliance

- 3.4 - Compliance artifact creation and delivery
- - 3.4.1 - Compliance artifacts

- 3.5 - Understanding open source community engagements
- - 3.5.1 - Contributions

- 3.6 - Adherence to the specification requirements
- - 3.6.1 - Conformance
- - 3.6.2 - Duration
```

Example Suggestion for ISO/IEC 5230:2020

```
## 2.7 - SPDX

the format standard created by the Linux Foundation's SPDX (Software Package Data Exchange)
Working Group for exchanging bill of materials for a given software package, including
associated license and copyright information (see [spdx.org](https://spdx.org/))
```

```
## 2.7 - software bill of materials (SBOM)

a “Software Bill of Materials” (SBOM) is a inventory for software, a list of ingredients that
make up software components. An example is the (Software Package Data Exchange) SPDX
specification created by the Linux Foundation's SPDX Project to exchange bill of materials for a
given software package (see spdx.org). Regardless of the SBOM specification used, it should
follow a complete profile for the intended use case.
```

THE LINUX FOUNDATION

OPENCHAIN

Example Suggestion for ISO/IEC 5230:2020

```
### 3.6.2 - Duration

A program that is OpenChain conformant with this version of the specification shall last 18
months from the date conformance validation was obtained. The conformance validation
registration procedure can be found on the OpenChain project's website.
```

```
### 3.6.2 - Duration

A Program that is conformant with this version of the specification will have a review period
every 12 months.
```

Review of suggested changes to ISO/IEC 18974:2023

- Current ISO standard:
  - https://github.com/OpenChain-Project/Security-Assurance-Specification/blob/main/Security-Assurance-Specification/ISO-18974/en/ISO-18974.md
- Current Next Generation Draft (pre-public comments period):
  - https://github.com/OpenChain-Project/Security-Assurance-Specification/blob/main/Security-Assurance-Specification/2.0/en/openchain-security-specification-2.0.md
- All open issues have been closed by the Specification Work Group
  - https://github.com/OpenChain-Project/Security-Assurance-Specification/issues?q=is%3Aissue+is%3Aclosed

Next:

- Six month public comment period launched 19h June 2024 as per our specification development process:
  - https://openchainproject.org/resources/faq#specification-development-questions
- This will be followed by a Three Month freeze period

Example Suggestion for ISO/IEC 18974:2023

```
#### 4.1.5 Standard practice implementation

The program shall demonstrate sound and robust handling procedures of known vulnerabilities and
secure software development by defining and implementing following procedures:

- Method to identify structural and technical threats to the supplied software;
- Method for detecting existence of known vulnerabilities in supplied software;
- Method for following up on identified known vulnerabilities;
- Method to communicate identified known vulnerabilities to customer base when warranted;
- Method for analyzing supplied software for newly published known vulnerabilities post release
of the supplied software;
- Method for continuous and repeated security testing to be applied for all supplied software
before release;
- Method to verify that identified risks will have been addressed before release of supplied
software;
- Method to export information about identified risks to third parties as appropriate.

A process shall exist for the security assurance methods listed above.
```

```
### 3.1.5 – Standard Practice Implementation

The Organization demonstrates sound procedures for handling Known Vulnerabilities and for
ensuring Secure Software Development by defining and implementing robust methods for:

- Identifying structural and technical threats to the Supplied Software;
- Detecting the existence of Known Vulnerabilities in the Supplied Software;
Monitoring the identified Known Vulnerabilities;
- Communicating the identified Known Vulnerabilities to customer base when warranted;
- Analyzing the Supplied Software for newly published Known Vulnerabilities post-release;
- Conducting continuous and repeated Security Testing for all Supplied Software before release;
- Verifying that the identified risks have been addressed before release of Supplied Software;
- Certifying that exported information about the identified risks to the third parties is
appropriate.

A process shall exist for the Security Assurance methods listed above.
```

Example Suggestion for ISO/IEC 18974:2023

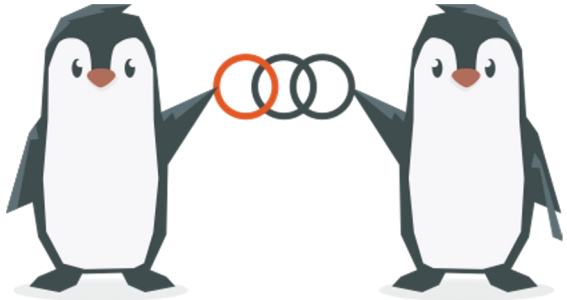
```
#### 4.4.2 Duration

A program that is OpenChain conformant with this version of the specification shall last 18
months from the date conformance validation was obtained. The conformance validation
registration procedure can be found on the OpenChain project's website.
```

```
### 3.4.2 - Duration

A Program that is conformant with this version of the specification will have a review period
every 12 months.
```

Other Important Things



Volvo Cars Announces Adoption of ISO/IEC 5230

VOLVO

THE LINUX FOUNDATION

OPENCHAIN

openEuler Adopts ISO/IEC 18974 + Case Study

openEuler

News

Case Study

THE LINUX FOUNDATION

OPENCHAIN

Socionext Recertification of ISO/IEC 5230

socionext™

THE LINUX FOUNDATION

OPENCHAIN

ISO/IEC 5230 Three-Way Case Study

BlackBerry

BlackBerry: Three-Way Case Study – The use of ISO/IEC 5230:2020 by a company providing mission-critical services to enterprise clients around the world

By Shane Coughlan | 2024-03-26 | Featured, News

BlackBerry, OSS Consultants and OpenChain

The OpenChain Project maintains two ISO/IEC standards designed to help optimize business process management around open-source software. One of the standards, ISO/IEC 5230:2020, focuses on how to establish and run a quality open-source license compliance program. Another of the standards, ISO/IEC 18974:2023, focuses on how to establish and run a quality open-source security assurance program. Taken together, these standards provide a reliable, efficient and effective way to manage the open-source supply chain.

This case study will highlight the use of ISO/IEC 5230:2020 by a company providing mission-critical services to enterprise clients around the world.

THE LINUX FOUNDATION

OPENCHAIN

Policy Briefing Series:

- EU Cyber Resilience Act
- EU AI Act
- EU Product Liability Directive

Ciarán O'Riordan
Senior Policy Advisor
OpenForum Europe (OFE)

THE LINUX FOUNDATION

OPENCHAIN

THE LINUX FOUNDATION

OPENCHAIN

AI Study Group Update

Workshops are held once a month discussing AI Compliance in the supply chain co-chaired by Matthew Crawford from Arm and David Marr from Qualcomm. It has identified some shared concerns across industries. **Potential emerging consensus for developing a guide to using AI BOM for building trust in the supply chain in 2H 2024.**

April

May

June

THE LINUX FOUNDATION

OPENCHAIN

OpenChain @ Events

OpenChain @ Open Source Summit North America
https://openchainproject.org/news/2024/04/17/openchain-open-source-summit-north-america-get-the-slides
OpenChain @ FINOS Open Source Readiness SIG
https://openchainproject.org/news/2024/05/02/openchain-finos-open-source-readiness-sig-2024-05-01
OpenChain @ LF Japan Executive Briefing
https://openchainproject.org/news/2024/05/14/openchain-lf-japan-executive-briefing
OpenChain @ AI Open Innovation Day 2024
https://openchainproject.org/news/2024/05/15/openchain-ai-open-innovation-day-2024
OpenChain Supply Chain Security & Compliance Workshop in Shenzhen
https://openchainproject.org/news/2024/05/22/supply-chain-security-compliance-may-2024
OpenChain @ International Open Source Trends For Industries in Taipei
https://openchainproject.org/news/2024/06/04/openchain-international-open-source-trends-for-industries-building-the-opensource-ecosystem-in-taiwan-2024-06-04
OpenChain @ OSBC Open Source Conference 2024
https://openchainproject.org/news/2024/06/16/coming-soon-openchain-osbc-open-source-conference-2024-2024-06-19

OpenChain Work Group Meetings

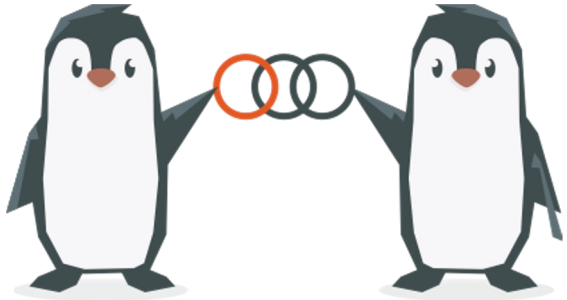
Key meetings that already happened:

- Korea Work Group Meeting #21, 26th March 2024
- Education Work Group in April, May and June
- Automation Work Group in April, May and June
- Telco Work Group in April, May and June
- Korea Work Group Meeting #22, 20th June 2024
- + Many Sub-Group meetings

Key meetings coming up:

- Japan Work Group Meeting #31, 27th June 2024
- China Work Group Regular Meeting #1, 28th June 2024
- Automotive Work Group Workshop - Announced for September

Important Changes the Board Decided



Current Study / Work Groups

Suggest to close: RED

Suggested to open: GREEN

Core Work Groups

Conformance (October 2016~)

Education (Autumn 2020~)

Specification (Spring 2016~)

Community Work Groups

Automation (Summer 2019~)

Export Control (Winter 2022~)

Legal Work Group (Winter 2022~)

Public Policy (Winter 2022~)

Community Study Groups

AI (January 2024~)

SBOM (July 2024~)

Industry-Specific Work Groups

Automotive (Summer 2019~)

Telco (Spring 2021~)

Regional User Groups

China (Sept 2019~)

Germany (Jan 2020~)

India (Sept 2019~)

Japan (Dec 2017~)

Korea (Jan 2019~)

Taiwan (Sept 2019~)

UK (June 2020~)

USA (June 2020~)

THE LINUX FOUNDATION

OPENCHAIN

Work Groups - Voted to Close

1. **Conformance Work Group**:
   send discussion to the Education Work Group and / or board as appropriate.
1. **Export Control Work Group**:
   send discussion to the main mailing list or the Governing Board as appropriate.
1. **Legal Work Group**:
   send discussion to the main mailing list or the Governing Board as appropriate.
   There is also the option of using outside activities for other topics in this domain:
   i. Linux Foundation member counsel calls,
   ii. the FSFE Legal and Licensing Workshop, and
   iii. the Open Compliance Summit in Japan.
1. **Public Policy Work Group**:
   send discussion to the main mailing list and / or board as appropriate.
1. **US Work Group**:
   send discussion to the main mailing list and / or board as appropriate.

Study Group – Voted to Open

- **SBOM Study Group**: focused discussion on **how to use** SBOM in the market.
    a. Use our learned experience in existing SBOM Sub-Groups, creating Telco SBOM Quality Guide and creating SPDX Lite.

Important point:

- Not working on a new SBOM Format
- Working on this question:
    - “What is a quality and practical approach for using SBOMs in the supply chain to support trusted compliance or security programs?”

Study / Work Groups After Board Decision

Main Work Groups

Education (Autumn 2020~)

Specification (Spring 2016~)

Community Work Groups

Tooling (Summer 2019~)

Community Study Groups

AI (January 2024~)

SBOM (June 2024~)

Industry-Specific Work Groups

Automotive (Summer 2019~)

Telco (Spring 2021~)

Regional User Groups

Japan (Dec 2017~)

Korea (Jan 2019~)

India (Sept 2019~)

China (Sept 2019~)

Taiwan (Sept 2019~)

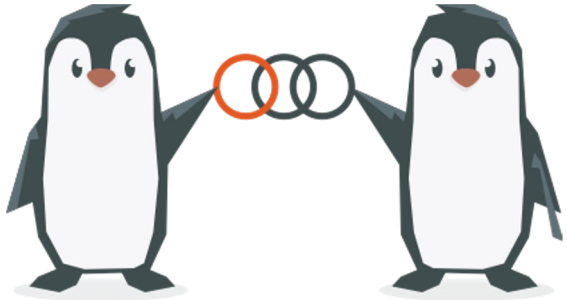
Germany (Jan 2020~)

UK (June 2020~)

THE LINUX FOUNDATION

OPENCHAIN

An Invitation to Japan Work Group (Planning SG)



Strategy Sub-Committee Update

OpenChain has a Governing Board Strategy Sub-Committee chaired by Matthew Crawford from Arm. It is hosting one hour reviews of Work Groups with the goal of better understanding community activity.

The first regular meeting involved an exploration of the activities of the **Education Work Group**.

Strategy Sub-Committee Update

The **OpenChain Japan Work Group, Planning Sub-Group** is invited to attend the next Strategy Sub-Committee meeting to give a presentation on:

- Past activities
- Current activities
- Ideas for the future
- Suggestions for how the OpenChain board can help support you

The date of the meeting is not decided, but it will be in Q3 2024.

Thank You!

Let’s build a better future for the trusted supply chain together

Let’s support the new generation with beginner and intermediate education

Let’s support the experienced community members with useful expert knowledge

THE LINUX FOUNDATION

OPENCHAIN