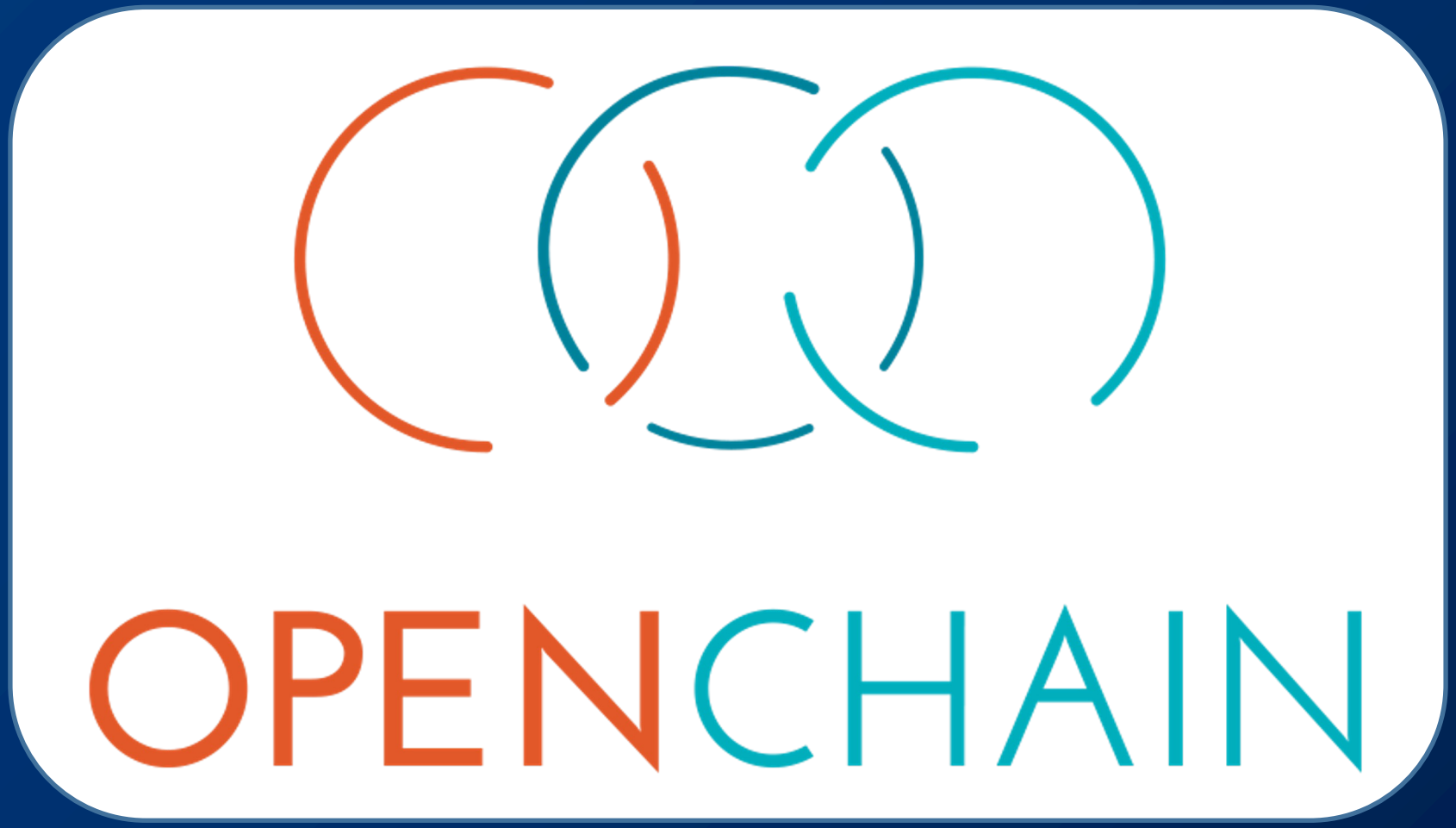


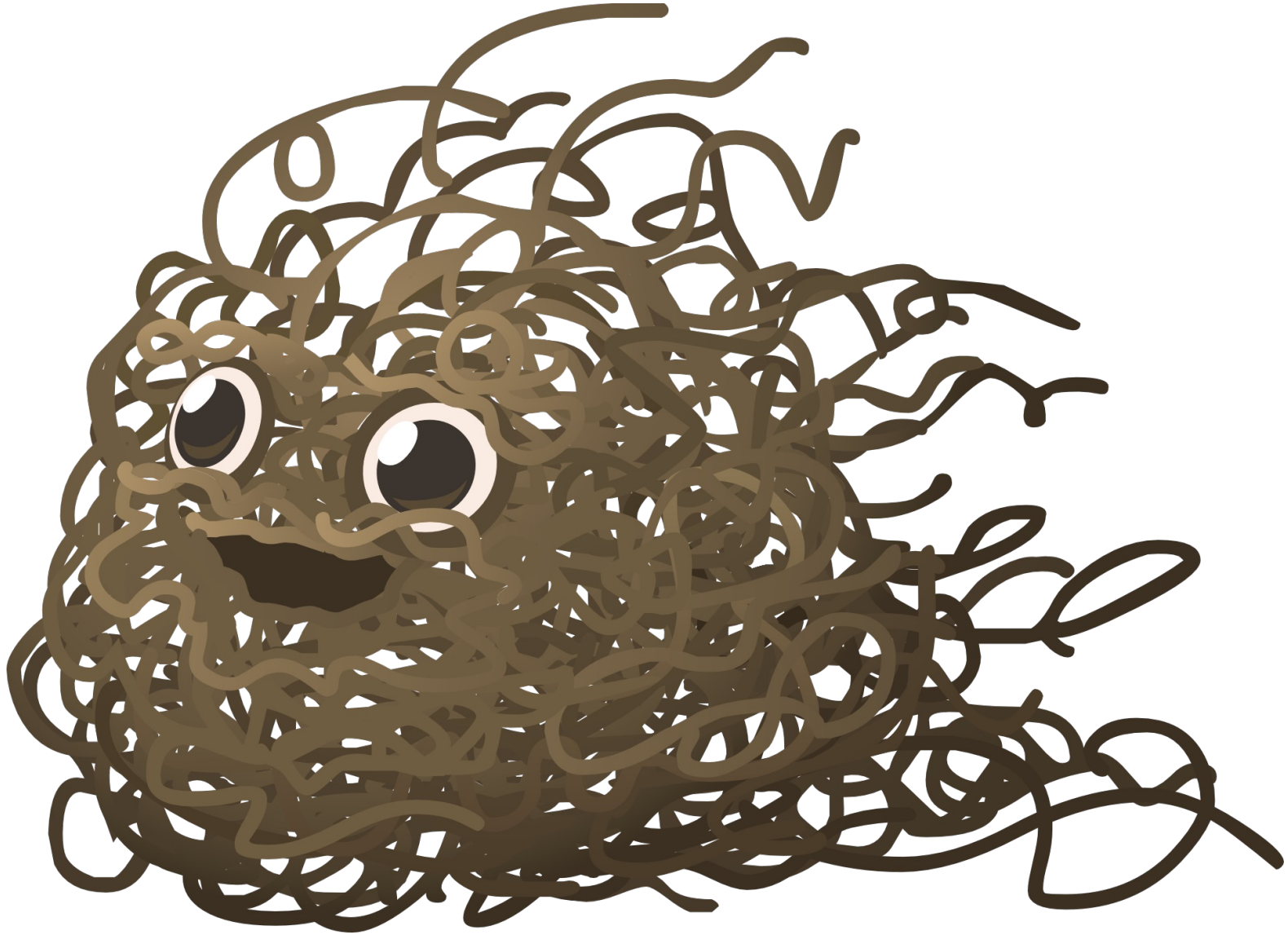
How The Linux Foundation Standards For License Compliance And Security Will Fix Your Supply Chain

Our Mental Model Of The Supply Chain

OPENCHAIN

The Actual Supply Chain

OPENCHAIN



OPENCHAIN

67.4%

of managers monitor their supply chain with Excel spreadsheets

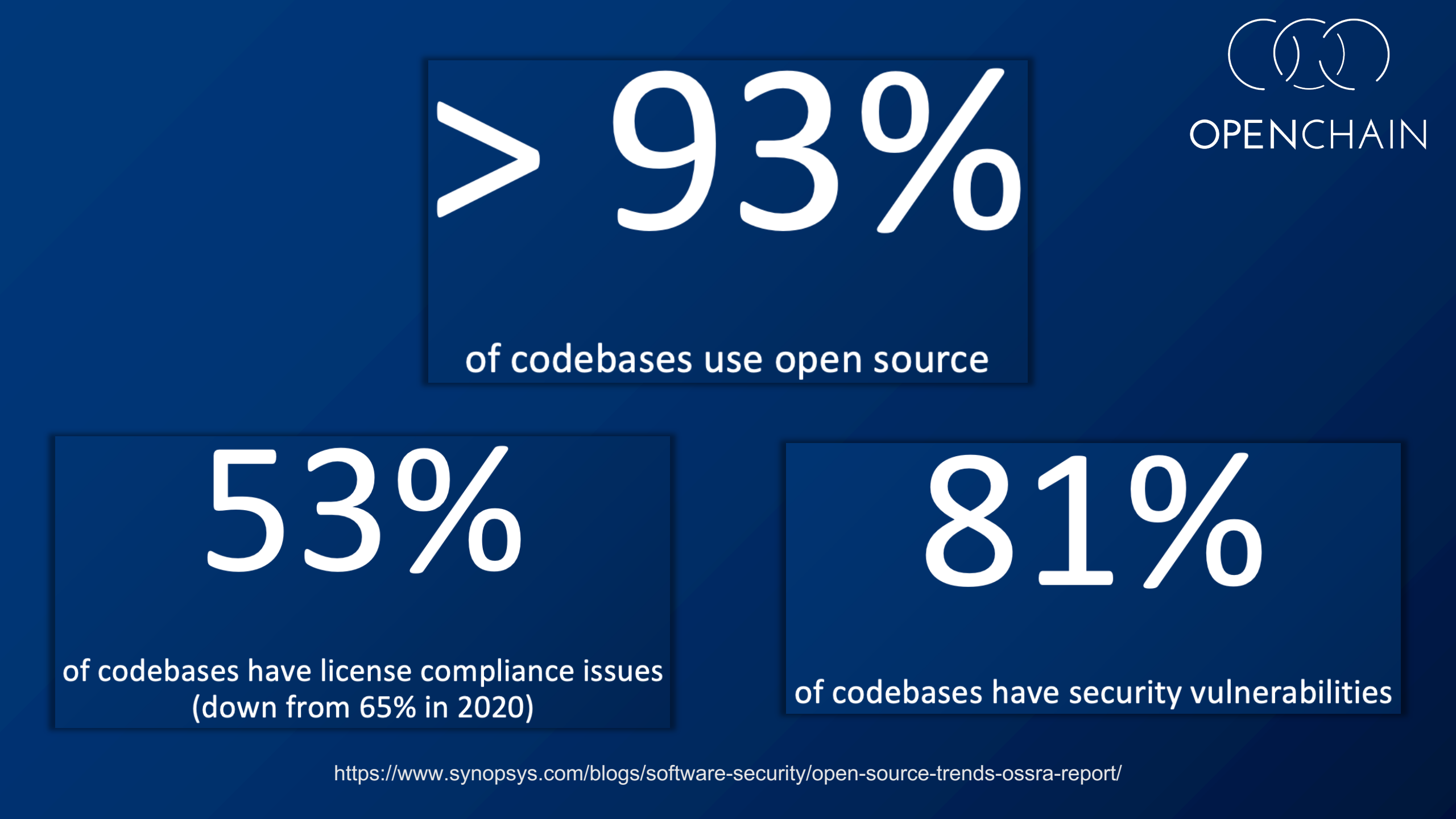
https://www.zippia.com/advice/supply-chain-statistics/

OPENCHAIN

94%

of companies do not have full visibility of their supply chain

https://www.zippia.com/advice/supply-chain-statistics/


OPENCHAIN
> 93%
of codebases use open source
53%
of codebases have license compliance issues
(down from 65% in 2020)
81%
of codebases have security vulnerabilities
https://www.synopsys.com/blogs/software-security/open-source-trends-ossra-report/

OPENCHAIN

40%

potential savings available via supply chain optimization

57%

of companies see supply chain management as a competitive edge

70%

of companies see supply chains as a driver for customer service

https://www.zippia.com/advice/supply-chain-statistics/

Context: This Is Important To Business

Open Source License Compliance and Security Assurance
is a key part of supply chain management.

We Got Together To Improve The Supply Chain

OPENCHAIN

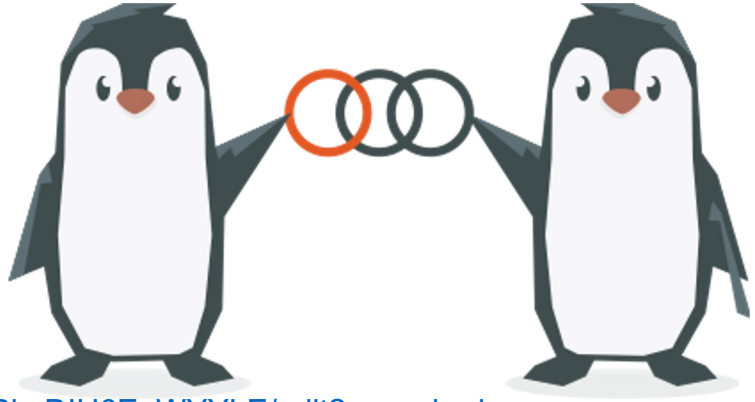
arm
BLOCK
BMW GROUP
BMW Car IT
BOSCH
CARIAD
A VOLKSWAGEN GROUP COMPANY
CISCO
COMCAST
ERICSSON
FUJITSU
Google
HITACHI
Inspire the Next
HONOR
HUAWEI
Meta
Microsoft
MOXA
NEC
oppo
Panasonic
Qualcomm
Qualcomm Technologies, Inc.
SIEMENS
SONY
TOSHIBA
TOYOTA
Uber

OpenChain Membership – New (old) Faces!

CARIAD

(not an official VW ID.4)

Members Represent Over 5.9 Trillion USD In Market Value



https://docs.google.com/spreadsheets/d/1HllBIFRkqiUc-6nnJWRkPd1VmiajeRknDIH6EnWYYLE/edit?usp=sharing

Broader Community

OPENCHAIN

Main Work Groups:

- Specification (Spring 2016~)
- Education (Autumn 2020~)

Community Work Groups:

- Tooling (Summer 2019~)
- Export Control (Winter 2022~)
- Public Policy (Winter 2022~)

Special Interest Groups:

- Automotive (Summer 2019~)
- Telecom (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~)
- USA (Dec 2020~)

Example Verticals Impacted by OpenChain

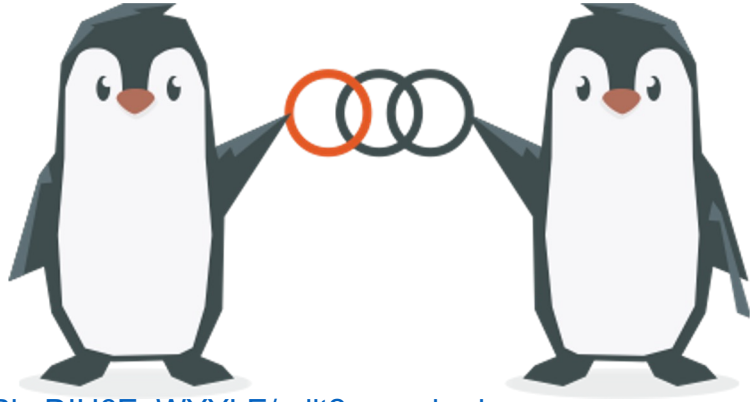
Automotive	Banking	Cloud	Consumer	Industrial	SaaS	Service	Silicon	Telco
BMW GROUP	BLOCK	Alibaba Cloud	HARMAN	FUJITSU	BlackBerry	Cognizant	arm	中国移动 China Mobile
BOSCH	kakaobank	CLOUDERA	HONOR	GE Digital	ByteDance	Hitachi Vantara	ASML	cisco
CARIAD	YOMA BANK	Google	LG	HITACHI	kakao	IBM	socionext	COMCAST
Hella Aglaia		Microsoft	oppo	MOXA	Meta	Infosys	Qualcomm	ERICSSON
HYUNDAI		QCT	Panasonic	SIEMENS	Nextcloud	Interneuron	Western Digital	HUAWEI
HYUNDAI AutoEver			SAMSUNG	TOSHIBA	SAP	LYRA		SK telecom
HYUNDAI MOBIS			SONY	NEC	Uber	revenera		
KIA			ZTE		zoom	SAMSUNG SDS		
SCANIA						SUSE		
TOYOTA								
woven by TOYOTA								
Z-ONE								

● Platinum Member / Conformance Pending ● Platinum Member + ISO/IEC 5230 Conformant ● ISO/IEC 5230 + DIS 18974 Conformant

This is a snapshot based on membership and select conformant organizations currently listed on our website. Total conformant numbers are far higher.

Example: PwC Survey shows 20% of companies in Germany with over 2,000 employees already used ISO/IEC 5230.

Snapshoot Represents Over 7.5 Trillion USD In Market Value



https://docs.google.com/spreadsheets/d/1HllBIFRkqiUc-6nnJWRkPd1VmiajeRknDIH6EnWYYLE/edit?usp=sharing

Trillions More In Market Value Touched

(Lockheed co-chairs our spec development)


This is a non-exhaustive list of participants on some of our community lists

OPENCHAIN

1,000+

Companies Working On A Better Supply Chain

Trust Built By Process Management

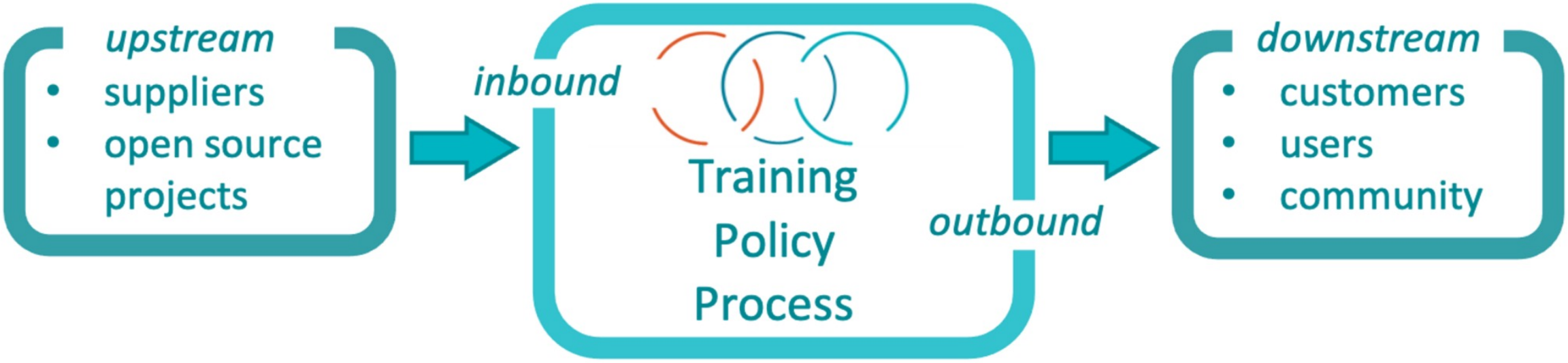
- **In Market Q4 2016~ (de facto) Q4 2020 (ISO/IEC)**
  OpenChain ISO/IEC 5230:2020
  The International Standard for open source license compliance.

- **In Market Q4 2022~ (de facto) Q3 2023 projected (ISO/IEC)**
  ISO/IEC DIS 18974, OpenChain Security Assurance Specification
  The de facto standard for open source security assurance compliance.

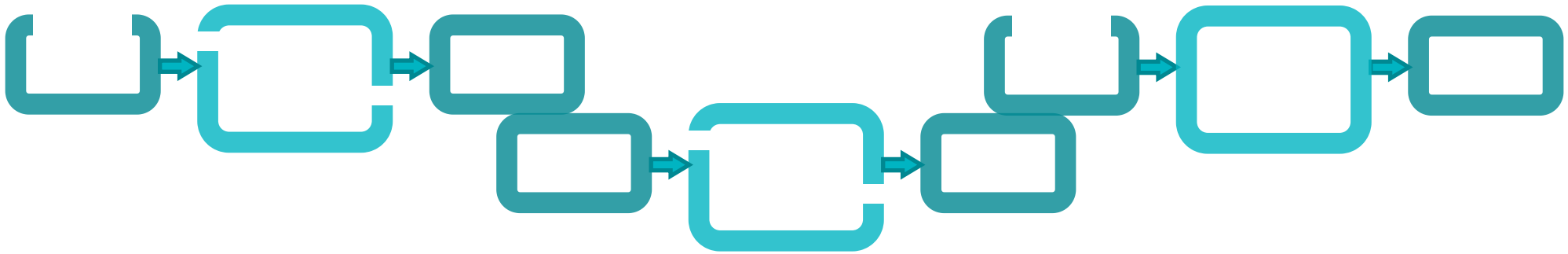
1. High level process standards;
2. Simple, effective and suitable for companies of all sizes in all markets;
3. Openly developed by a vibrant user community and freely available to all.

The Standards Work Company By Company

OPENCHAIN



Result = A More Predictable Supply Chain



OpenChain Has 98 ISO/IEC 5230 Conformant Orgs Listed On Our Website (totals are higher)

THE LINUX FOUNDATION

OPENCHAIN

Total conformant numbers are far higher.

Example: PwC Survey shows 20% of companies in Germany with over 2,000 employees already used ISO/IEC 5230.

20%

of German companies with over 2,000 employees
already use OpenChain ISO/IEC 5230

https://www.pwc.de/en/digitale-transformation/pwc-bitkom-study-open-source-monitor-2021.pdf

Recent Significant ISO/IEC 5230 Conformance

Momentum Is Growing Around ISO/IEC DIS 18974

- We expect to complete the Draft International Standard (DIS) process via JTC-1 at the end of June.
- There will be an editorial period after this.
- According to Seth from Joint Development Foundation:

"We will most likely end up passing with edits. We will clean up the editorial things but nothing technically normative and send it back. They will spend another month transposing the final version and give us the ISO number."

Conformance Continues With De-Facto Standard

LG

Life's Good

BlackBerry

Interneuron

Freedom Of Choice In Using Our Standards

OPENCHAIN

1. Self-Certification
2. Independent Assessment
3. Third-Party Certification

Free Self-Certification Material

OPENCHAIN

Section 1: Program foundation

- [ ] We have a policy governing the open source license compliance of Supplied Software.
- [ ] We have a documented procedure to communicate the existence of the open source policy to all Software Staff.
- [ ] We have identified the roles and responsibilities that affect the performance and effectiveness of the Program.
- [ ] We have identified and documented the competencies required for each role.
- [ ] We have documented the assessed competence for each Program participant.
- [ ] We have documented the awareness of our Program participants on the following topics:
  - [ ] The open source policy and where to find it;
  - [ ] Relevant open source objectives;
  - [ ] Contributions expected to ensure the effectiveness of the Program;
  - [ ] The implications of failing to follow the Program requirements.
- [ ] We have a process for determining the scope of our Program.
- [ ] We have a written statement clearly defining the scope and limits of the Program.
- [ ] We have a documented procedure to review and document open source license obligations, restrictions and rights.

Section 2: Relevant tasks defined and supported

- [ ] We assigned individual(s) responsibility for receiving external open source compliance inquiries.
- [ ] The external open source compliance contact is publicly identified (e.g. via an email address or the Linux Foundation Open Compliance Directory).
- [ ] We have a documented procedure for receiving and responding to open source compliance inquiries.
- [ ] We have documented the persons, group or function supporting the Program role(s) identified.
- [ ] We have ensured identified Program roles been properly staffed and adequately funded.
- [ ] Legal expertise to address internal and external open source compliance has been identified.
- [ ] We have a documented procedure assigning internal responsibilities for open source compliance.

OpenChain Has 11 Official Third-Party Certifiers

OpenChain Has 27 Official Service Providers

THE LINUX FOUNDATION

OPENCHAIN

OpenChain Has 22 Official Legal Providers

ARRAY

ATOUT [PI] LAPLACE GROUPE VIDON

BAKER BOTTS

bkl BAE, KIM & LEE LLC

C/M/S/ Law.Tax

fieldfisher

GTC LAWYERS + STRATEGISTS

HAMILTON BROOK SMITH REYNOLDS Intellectual Property Law

HH PARTNERS ATTORNEYS-AT-LAW

id est avocats

id law partners

JBB

理慈 Lee, Tsai & Partners

Lex Pan Law™

MCA

MOORCROFTS CORPORATE LAW

Osborne Clarke

South Toranomon Law Offices

StudioLegale.it

taylor | english

WITZEL ERB BACKU & PARTNER

THE LINUX FOUNDATION

OPENCHAIN

OpenChain Has 12 Official Tooling Vendors

Example Reference Material - Online Training

OPENCHAIN

Introduction to Open Source License Compliance Management (LFC193)

Implementing Open Source License Compliance Management (LFC194)

1. LFC193 - 1209 total enrollments (398 digital badges issued)
   4.65 out of 5 rating by users
2. LFC194 - 579 total enrollments (138 digital badges issued)
   4.55 out of 5 rating by users

Example Of Market Use

OPENCHAIN

Continental ♥ Introduction to Open Source License Compliance Management (LFC193)

Continental made LFC193 a required course for their software developers from late Q3

BOSCH ♥ Introduction to Open Source License Compliance Management (LFC193)

Bosch has asked suppliers and requires external developers to use LFC193 since Q4 2021

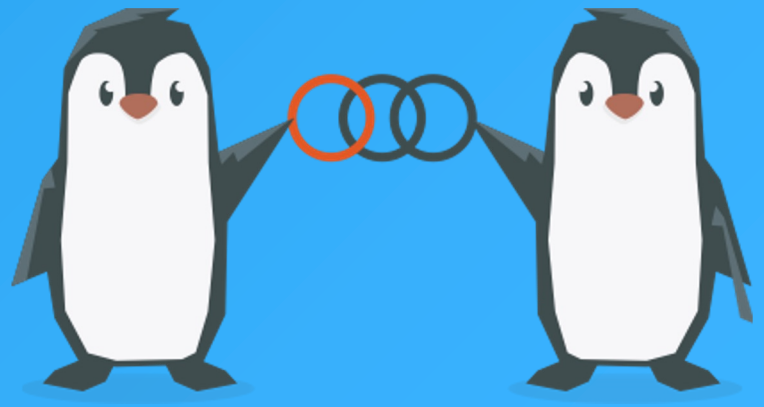
KPMG ♥ Introduction to Open Source License Compliance Management (LFC193)

KPMG AG asks their developers and architects to complete LFC193

What Else Is Happening?

THE LINUX FOUNDATION

OPENCHAIN



General Community News: Project Improvements

ISO/IEC 5230 One Pager Updated

By Shane Coughlan | 2023-03-09 | Featured, News

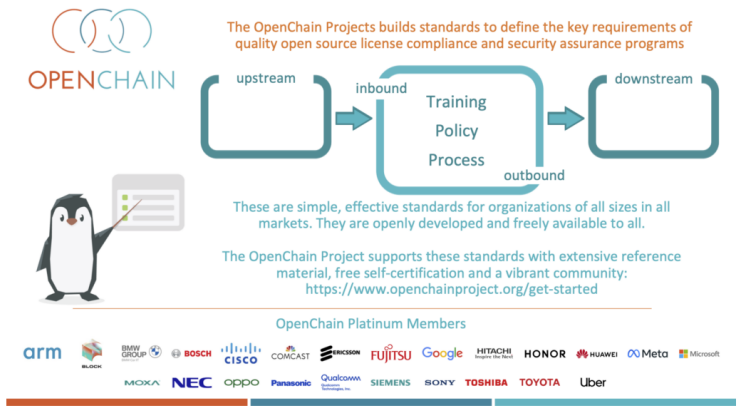
The ISO/IEC 5230 one page overview has been updated to provide simple, clear messaging about how and why the International Standard for open source license compliance provides value to companies in the supply chain.

This document is available in PDF format, PNG format or InDesign format. You may take it, use it, share it and remix it freely using the terms of the CC0 license, effectively public domain.

You can help us improve this document, translate it and convert it into new formats through the OpenChain GitHub Reference Library. We are actively seeking a MarkDown version for ease of future iteration.

OpenChain Project One Slide Overview Updated

By Shane Coughlan | 2023-03-10 | Featured, News

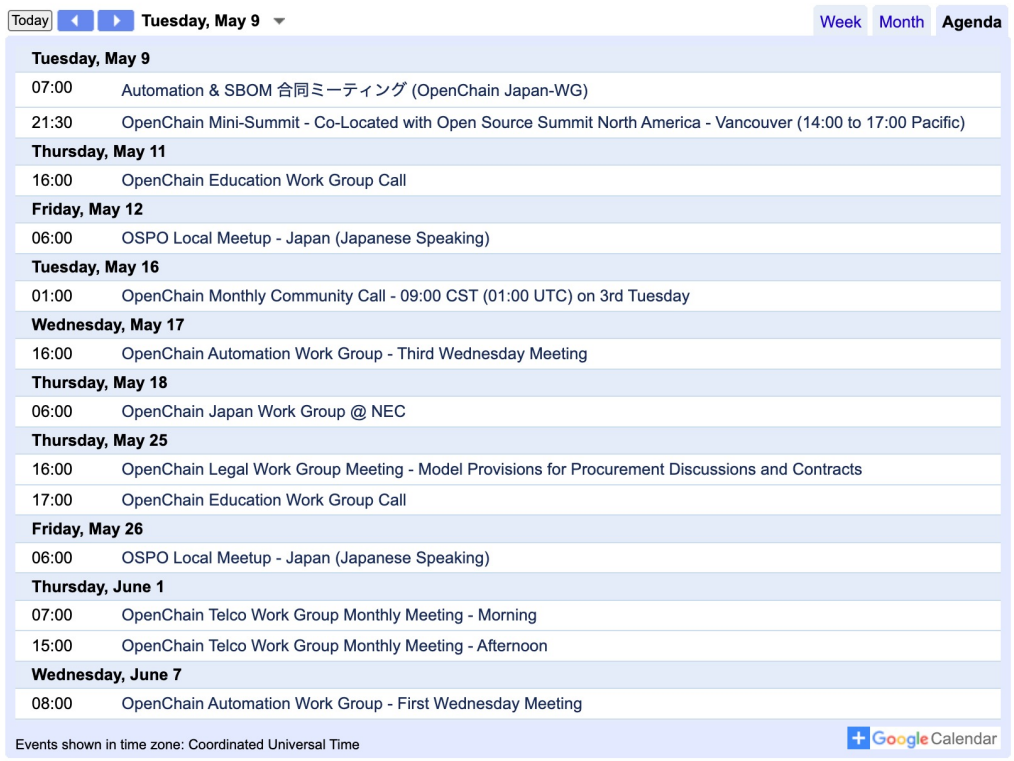


The one slide overview of the OpenChain Project has been updated to provide simple, clear messaging about how and why our work provides value to companies in the supply chain.

General Community News: Project Improvements

Improved OpenChain Community Calendar

By Shane Coughlan | 2023-02-27 | News

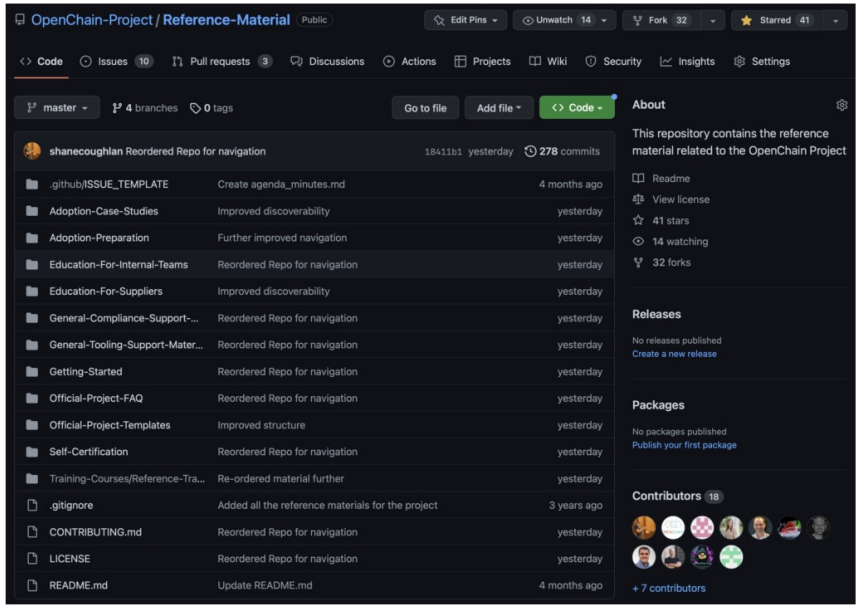


The OpenChain Community Calendar has been revamped to make it much easier to find and attend our events. The new calendar view is in list format and is now present on both our landing page and our participation page.

General Community News: Project Improvements

OpenChain Reference Library – Complete Overhaul

By Shane Coughlan | 2023-02-24 | Featured, News



The OpenChain Reference Library has been significantly updated to improve navigation. This is an administrative item that was pending for a while. Its completion should make it possible (and easy!) for anyone to access our library and find material. It should also make it a lot easier for our Education Work Group to assess and improve or expand existing material.

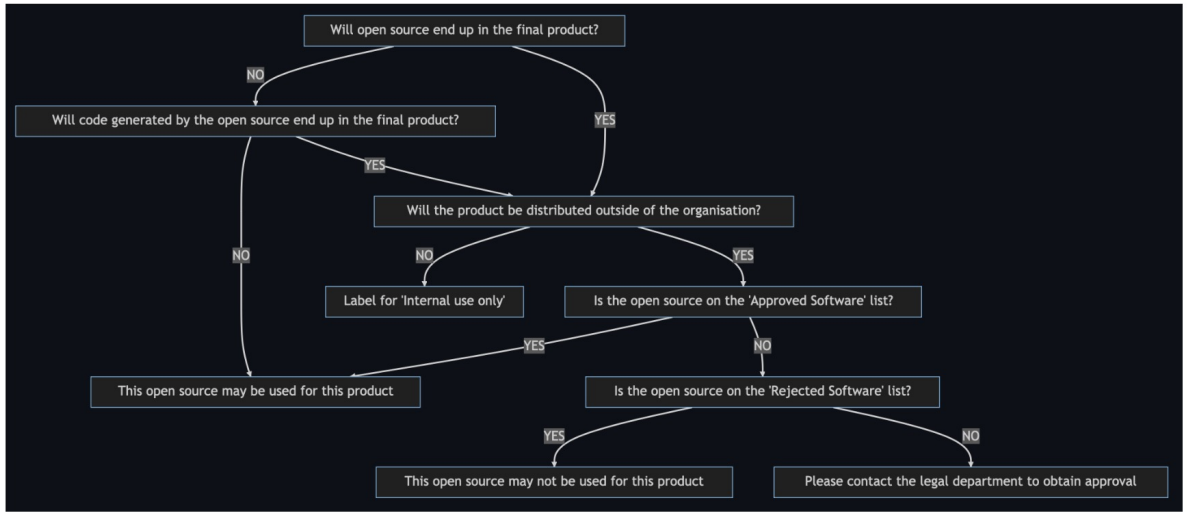
General Community News: Project Activities

GPLv2 Compliance Flowcharts Updated

By Shane Coughlan | 2023-04-13 | News

The OpenChain Project GPLv2 Compliance Flowcharts have been updated. Originally published in the book Practical GPL Compliance, these flowcharts are intended to help address some common compliance workflows. Thanks to Jacob Wilson, they have been moved into MarkDown format, and can now be easily added to websites, elearning platforms and more.

Example: Flowchart #0 – How Do I Distribute

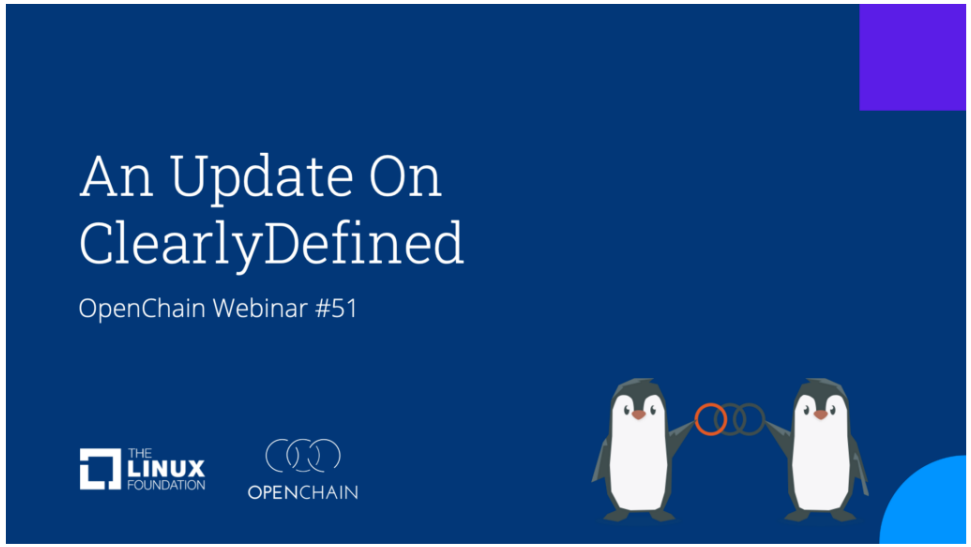


You can access and download these flowcharts in our Reference Library. Like the rest of our material, they are released under CC-0 licensing.

General Community News: Webinars

OpenChain Webinar #51 – An Update On ClearlyDefined

By Shane Coughlan | 2023-04-26 | News, Webinar



OpenChain Webinar #51 featured an update on ClearlyDefined by Nick Vidal at the Open Source Initiative (OSI). A lot has happened since we last covered this project for open source metadata, including the move to a new home at OSI.

General Community News: Events

OpenChain @ Legal and Licensing Workshop 2023 – Gothenburg, Sweden – 2023-04-21

By Shane Coughlan | 2023-04-21 | News

The OpenChain Project was featured at the FSFE Legal and Licensing Workshop 2023 held in Gothenburg, Sweden during April. This annual event brings together legal experts from around the world to talk about open source and open-related legal matters.

OpenChain @ 2nd China Automotive Cyber Security and Data Security Conference 2023

By Shane Coughlan | 2023-04-20 | News

The OpenChain Project has been featured at the 2nd China Automotive Cyber Security and Data Security Conference 2023 in a talk delivered by Zhang JunXia of CAICT. This is part of our long-running collaboration to help companies of all sizes in the Chinese market to adopt and use ISO/IEC 5230, the international standard for open source license compliance.

General Community News: Publications

OpenChain ISO/IEC Featured In Journal Of Software (软件学报)

By Shane Coughlan | 2023-03-13 | Featured, News

OpenChain ISO/IEC 5230:2020 is featured positively in the 'Survey on Open-source Software Supply Chain Security' published in the Journal Of Software (软件学报) Volume 33, Issue 3, 2023.

This article by JI Shou-Ling, WANG Qin-Ying, CHEN An-Ying, ZHAO Bin-Bin, YE Tong, ZHANG Xu-Hong, WU Jing-Zheng, LI Yun, YIN Jian-Wei and WU Yan-Jun is worth reading in full for insight from a key market space for open source.

General Community News: Asking Questions

OpenChain Industry Survey 2023

By Shane Coughlan | 2023-04-03 | Featured, News

The OpenChain Industry Survey 2023 is now online.

Our annual OpenChain Industry Survey covers a big topic: the global status of corporate engagement and management of open source. It focuses on a 'strategy' perspective rather than a 'development' perspective. Our goal is to help inform corporate project, product and supply chain decisions in the year ahead.

Licensing and Security Specification Editing

- The editing process is continuing as expected, with solid feedback on issues, and changes heading in the direction of improved clarity.
- The open and closed issues are tracked via GitHub:
  Licensing: https://github.com/OpenChain-Project/License-Compliance-Specification/issues
  Security: https://github.com/OpenChain-Project/Security-Assurance-Specification/issues
- The draft next generation specifications are also hosted on GitHub:
  Licensing: https://github.com/OpenChain-Project/License-Compliance-Specification/blob/master/3.0/en/openchain-license-compliance-3.0.md
  Security: https://github.com/OpenChain-Project/Security-Assurance-Specification/blob/main/Security-Assurance-Specification/2.0/en/openchain-security-specification-2.0.md
- As are the slides used for every meeting (two meetings per month):
  https://github.com/OpenChain-Project/Meeting-Minutes/tree/main/Slides

Model Language For Procurement

- The first meeting of the Legal Work Group took place on the 25th of April 2023.
- We explored model provisions for including OpenChain ISO/IEC 5230 and OpenChain ISO/IEC DIS 18974 (and potentially other standards) in procurement contracts or similar material. The goal is to ensure people can understand options. We will not be prescriptive, and these model provisions will remain part of the OpenChain reference material. They will not be included in the standards themselves.
  - The call started by looking at model provisions done before via the Risk Grid.
  - The document, under public domain, has been moved to the OpenChain GitHub for ease of access and editing.
- Our outcome was to use this basic format to structure our first round of model provisions, and to have the option of merging the documents in the future.

THE LINUX FOUNDATION

OPENCHAIN

Learn more: https://www.openchainproject.org/news/2023/05/15/2nd-meeting-legal-wg

Be Part Of This

OPENCHAIN

https://www.openchainproject.org/participate