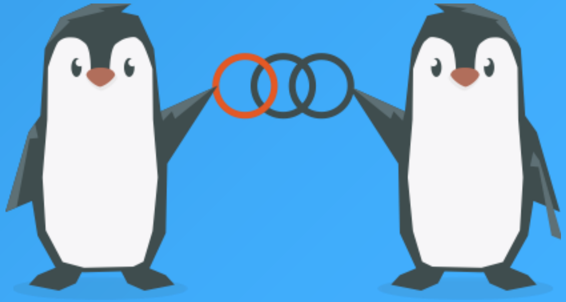
OpenChain Project

Understanding How We Build A More Trusted Open Source Supply Chain

THE LINUX FOUNDATION

OPENCHAIN



OpenChain Vision + Mission

Our vision is a trusted supply chain and our mission is to make that happen.

The purpose of the OpenChain Project is to align industry around standardized approaches to process management. This is to reduce risk, reduce costs and increase speed.

We create trust by improving compliance. We started with license compliance and expanded into security compliance. Our execution mechanism is normalization (community) and embedding (procurement).

Everything we have created – standards, community and reference material – is in service of our purpose and our mission.

Project Charter:
https://github.com/OpenChain-Project/Project-Charter-And-Agreements/blob/master/Project-Charter/OpenChain-Charter-March2020.pdf

Platinum Members (Governing Board)

amazon
arm
BMW GROUP
BMW Car IT
BOSCH
ByteDance
CARIAD
A VOLKSWAGEN GROUP COMPANY
CISCO

COMCAST
ERICSSON
FUJITSU
Google
HITACHI
Inspire the Next
HONDA
The Power of Dreams
HONOR

HUAWEI
Meta
Microsoft
MOXA
NEC
Panasonic
Qualcomm
Qualcomm Technologies, Inc.

SIEMENS
SONY
TOSHIBA
TOYOTA

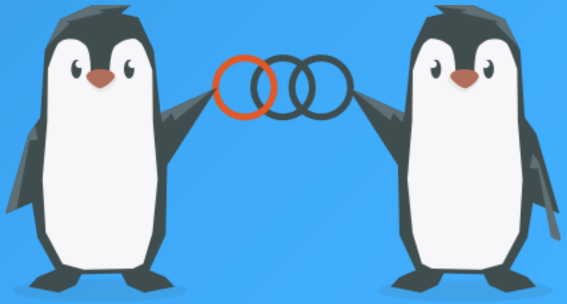
Members Represent Trillions In USD Market Value

THE LINUX FOUNDATION
OPENCHAIN

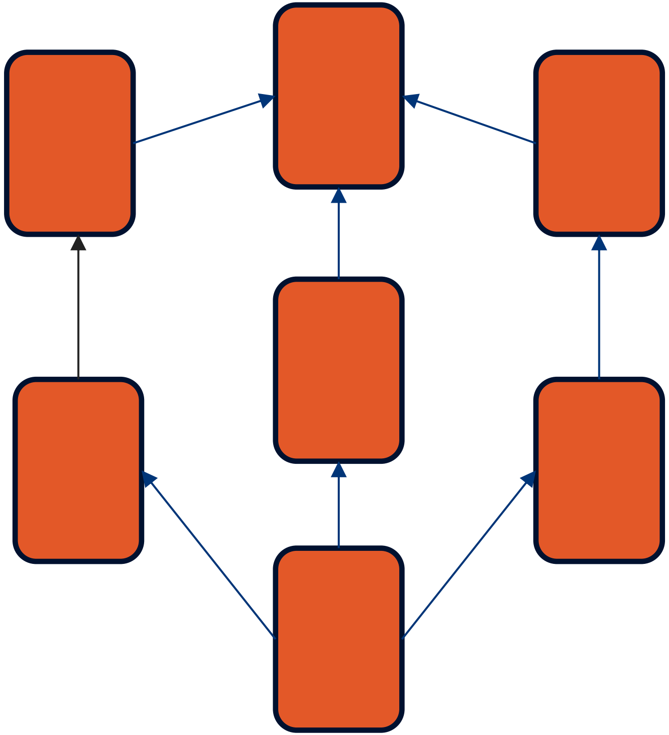
Project Overview

THE LINUX FOUNDATION

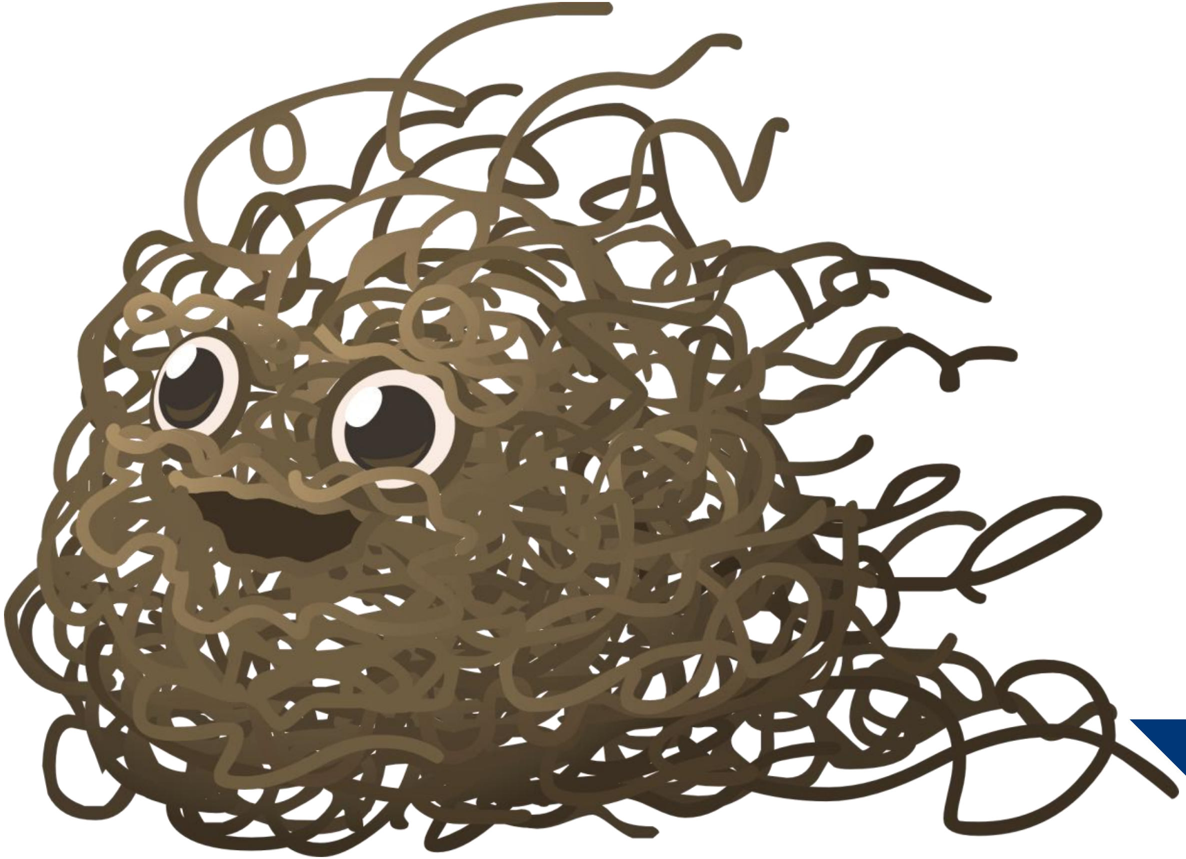
OPENCHAIN



Our Mental Model Of The Supply Chain



The Actual Supply Chain

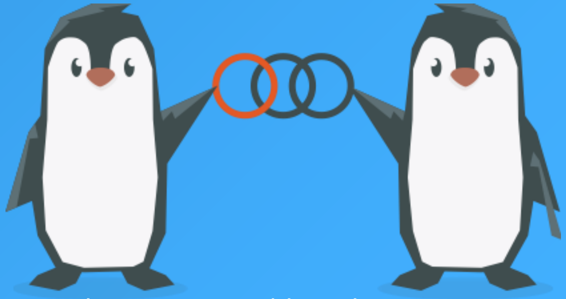


Global Codebase Statistics

Over 93% use open source

53% have license compliance issues

81% have security issues

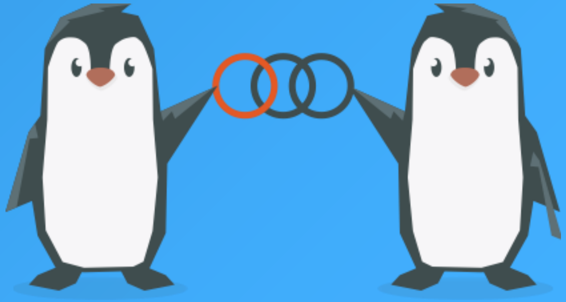


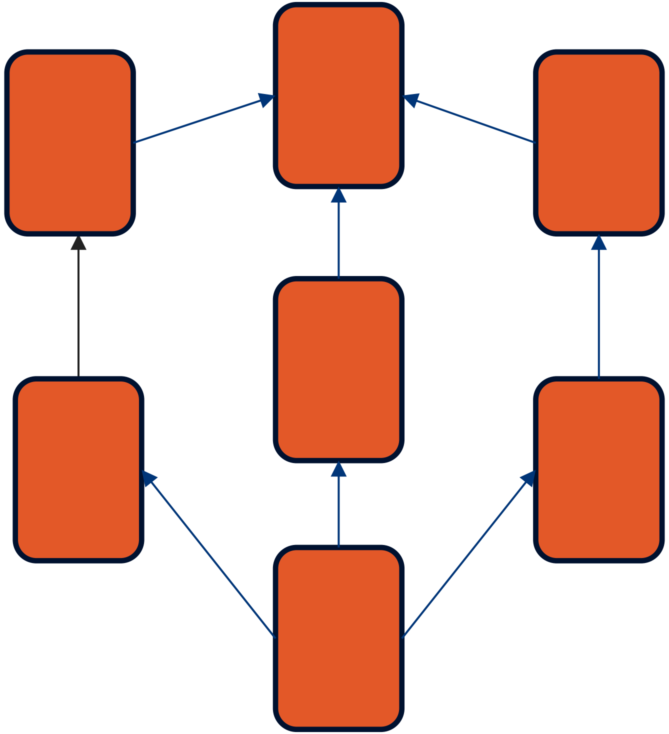
THE LINUX FOUNDATION

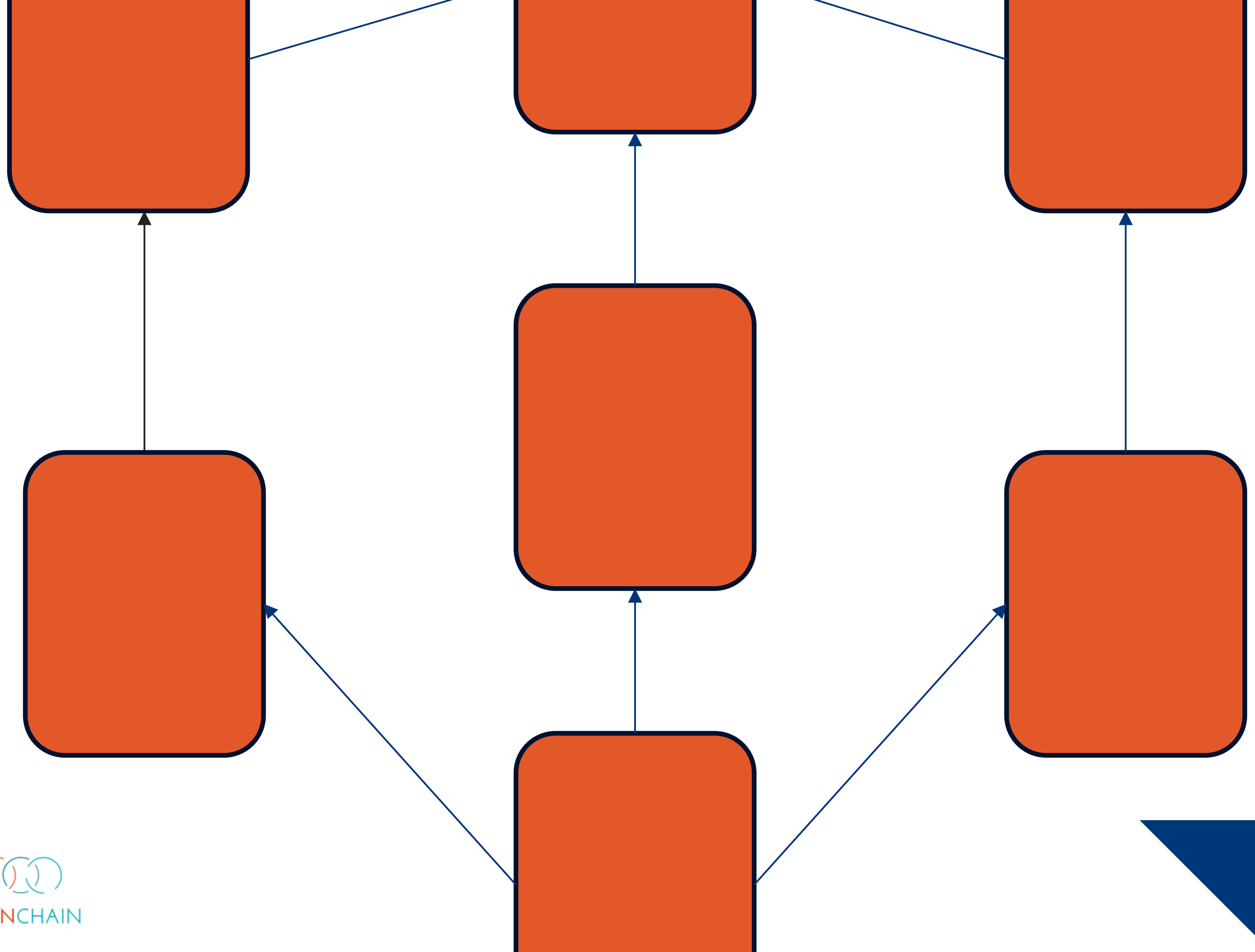
OPENCHAIN

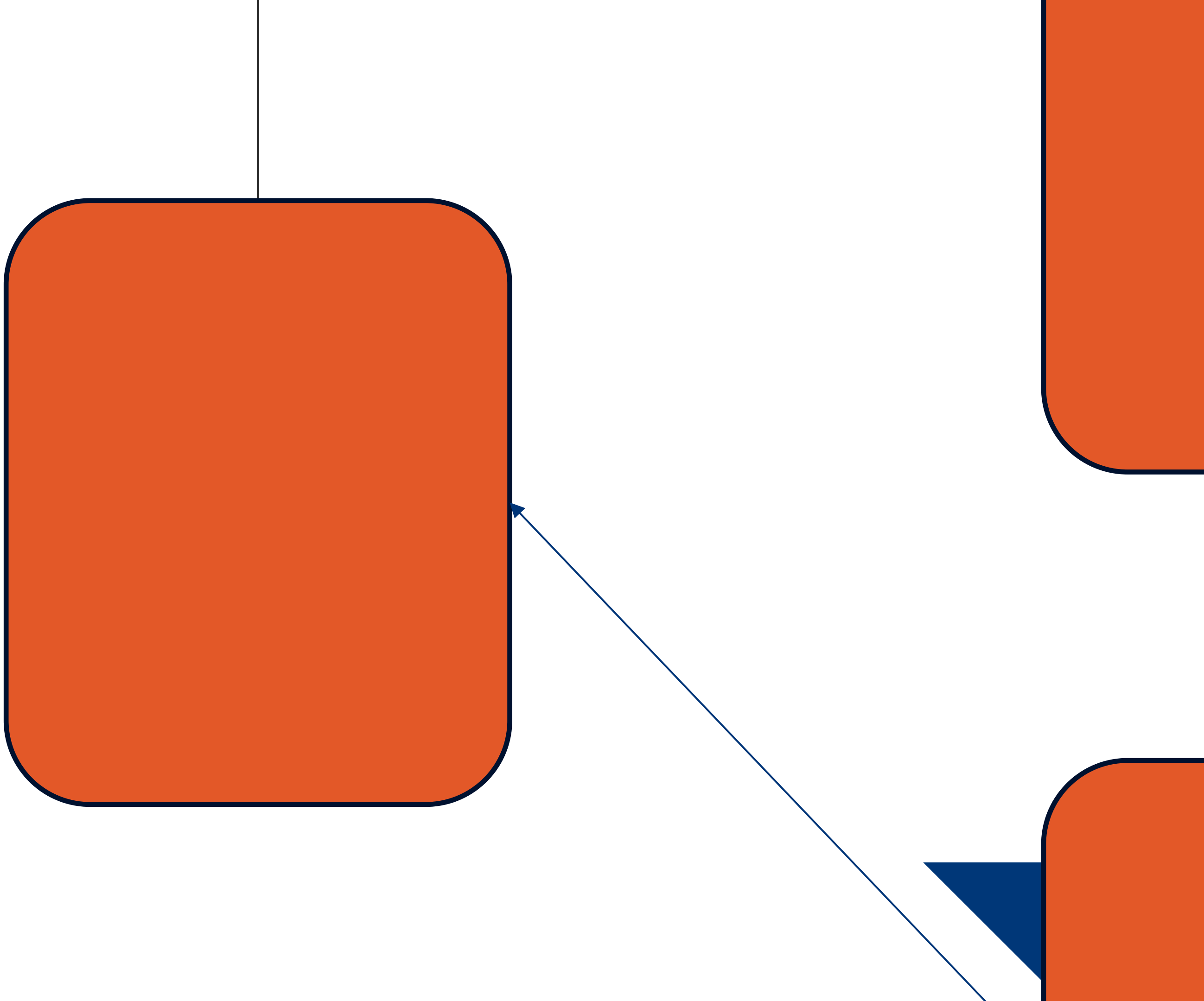
https://www.synopsys.com/blogs/software-security/open-source-trends-ossra-report/ (2022)

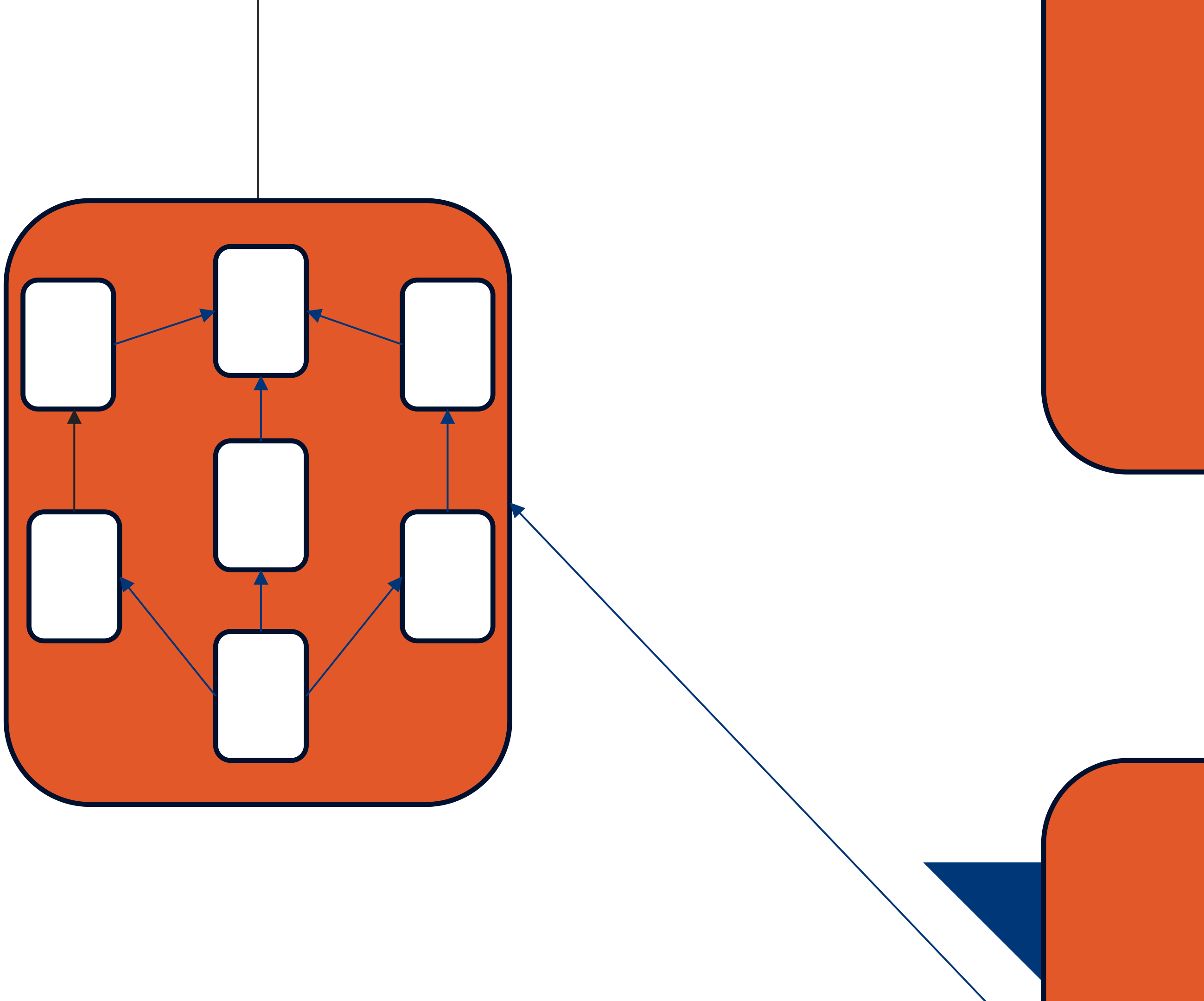
Not All Supply Chains Are External

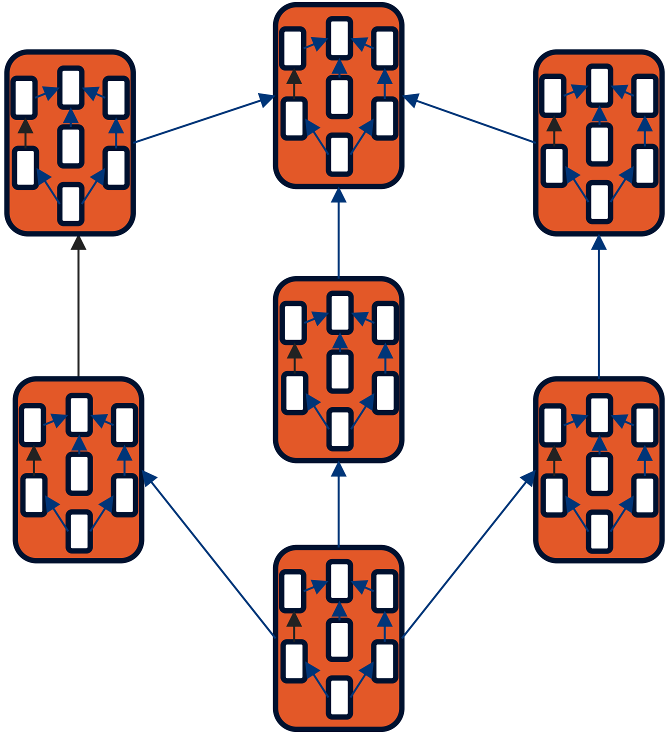








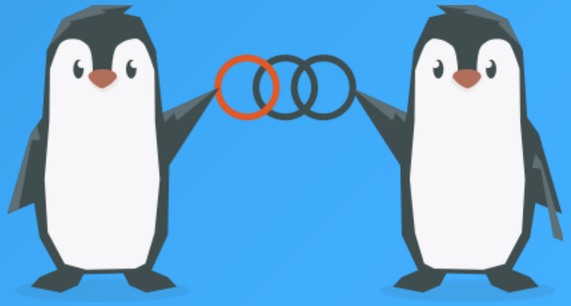




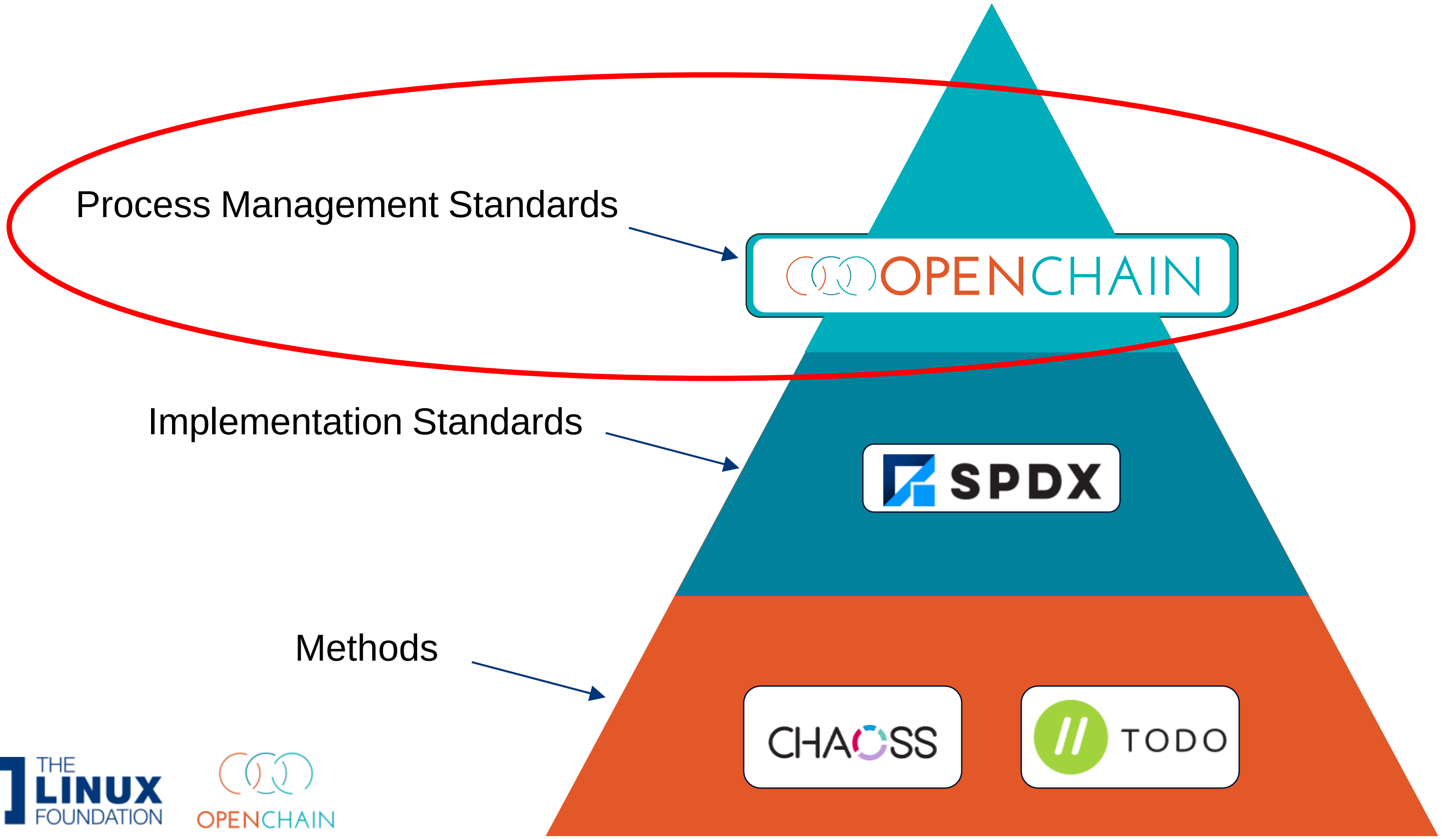
Internal / External… They are all the Supply Chain

THE LINUX FOUNDATION

OPENCHAIN



High Level Solution – Process Approach



Process Management Standards

Implementation Standards

Methods

Trust Built By Process Management

OpenChain ISO/IEC 5230:2020

International Standard for open source license compliance.

OpenChain ISO/IEC 18974:2023

International Standard for open source security assurance.

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

Sister Standards - Processes for Programs

ISO/IEC 5230 (License Compliance)

ISO/IEC 18974 (Security Assurance)

Flexible program size

Covering:

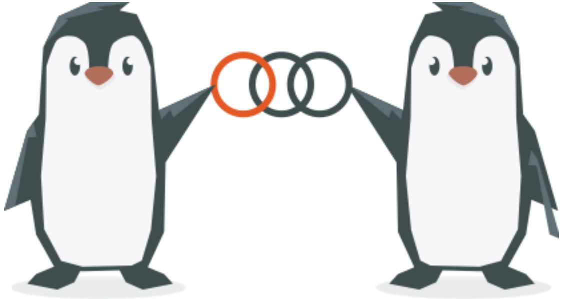
- Inbound processes
- Internal processes
- Outbound processes

Standards about process ***points***

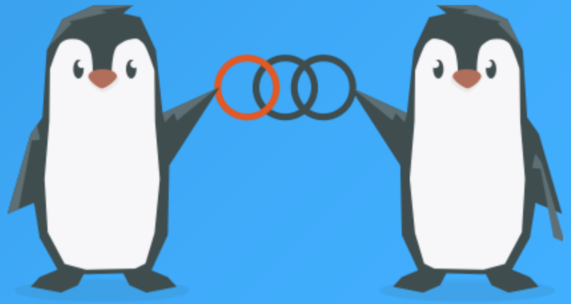
Not about process ***content***

ISO standards are a reputable shorthand in discussions, negotiations and contracts, allowing everything from “expected structure” to “what is a quality program” to be communicated easily.

The OpenChain standards are the *international baseline* for quality in open source license compliance or security assurance programs.



Progress Around Our Standards



A Continual Heartbeat Of Adoption

OpenChain standards are built, used and supported by all industries

Recent adoption announcements:

NOKIA

HARMAN
A SAMSUNG COMPANY

FUJITSU

SAMSUNG SDS

HONDA
The Power of Dreams

ISO/IEC 5230:2020

Alibaba Cloud
APTIV
arm
ASML
B2M SOLUTIONS
BangDB
BlackBerry
Bobble AI
BOSCH
ByteDance
CENLAB
China Mobile
CIRCLE
CISCO
CLOUDERA
Codewise
Cognizant
COLLABORA
Computermind
CODNTEC
CP1
credativ
CSI
dotcal
dSPACE
ECLIPSE FOUNDATION
emlix
ENDOCODE
ETRI
FINOVACE
FUJITSU
GE Digital
GBASE 南大通用
Google
H3C
HARMAN
Hella Aglaia
HENSOLDT
HITACHI
Hitachi Vantara
HONDA
HYUNDAI
HYUNDAI AutoEver
HYUNDAI MOBIS
IAV
IBM
Infosys
inno CUBE
Intelligence Node
Interneuron
inwinSTACK
kakao
kakaobank
KEITARO
KIA
KKCOMPANY
kt
LG
Liferay
LINE
LSware
Lyo
Microsoft
NAVER
NC
NEC
Nextcloud
NODEWEAVER
NOKIA
numbers
OPEN SOURCE SECURITY
OpenEuler
OpenHarmony
oppo
PELAGICORE
平凯星辰
QCT
Qualcomm
revenera
零束 ZONE
SAMSUNG
SAMSUNG SDS
SAP
SCANIA
SECTOR 7G
Shareablee
SIEMENS
SIEMENS Healthineers
SK telecom
socionext
软安科技
SONY
SOURCE Auditor
Source Code Control
SUSE
棱镜七彩
Synology
ToganLabs
TOSHIBA
TOYOTA
Uber
ura
Visteon
VOLVO
Western Digital
WIND
woven by TOYOTA
xFUSION
Яндекс
YES security
YOMA BANK
zoom
ZTE

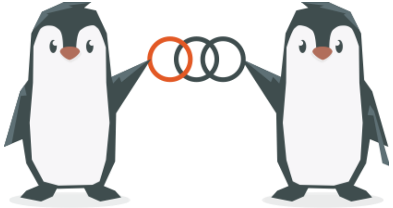
ISO/IEC 18974:2023

BlackBerry
CANOPUS
emlix
FUJITSU
HONDA
Interneuron
kakaobank
kt
LG
OpenEuler
revenera
SAMSUNG SDS

THE LINUX FOUNDATION

OPENCHAIN

Reminder: ISO standards can be adopted and used by any party, so we only get informed and do PR on a discretionary basis.



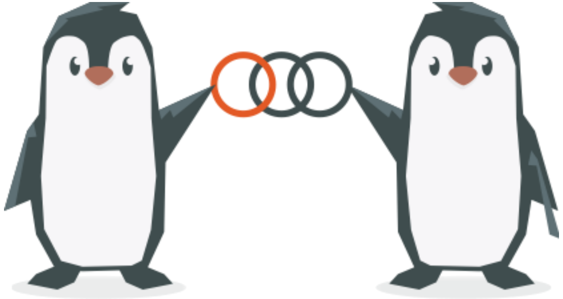
Data Point

31%

of large German companies already use or plan to adopt OpenChain ISO/IEC 5230

Source PwC: https://tinyurl.com/openchain-germany-31

ZF has announced an OpenChain ISO/IEC 5230 conformant program



ZF Third-Party Certification Process

ZF is a global leader in driveline, chassis, and safety technology, focusing on electrification and autonomy.

Challenges

- ISO 5230 maintenance
- Secure open source
- Process improvement
- Compliance management

Support by TIMETOACT

PART OF TIMETOACT GROUP

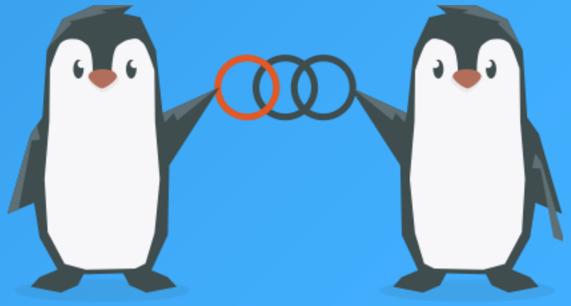
- **Maturity analysis**
  Evaluation of current open-source compliance
- **Gap analysis and closure**
  Identification and closing of compliance gaps
- **Audit and ISO/IEC 5230 certification** Support by ARS for auditing and certification

Results and Added Values

- Final audit rating of 90%
- **ISO/IEC 5230 certification** achieved in record time
- Strengthening of industry **image** and risk minimization
- Improved internal **efficiency** and strong awareness for open-source compliance
- Improved **quality standards**
- International recognition and competitive **advantages**
- Increased operational efficiency and **risk reduction**

ISO 5230

Adoption Methods



How Are OpenChain Standards Adopted?

- There are several mechanisms for the adoption of OpenChain Standards
- The most common way is self-certification
- Another way is third-party certification

Self-Certification – Rationale and Effectiveness

- Self-certification to an OpenChain standard (and any other standard) involves an entity reviewing material, deciding that they meet the requirements it describes, and then advertising that fact.

- OpenChain provides extensive resources to help with this, such as self-certification checklists.

- The OpenChain standards are explicitly designed to work effectively with self-certification because:
    - They require a company to keep records of how they certified and details of each point (verification materials)
    - They are designed for supply chain procurement, with an expectation that customer companies can and will audit supplier company verification materials at the time of their choosing

- This has proven effective, and no purposeful attempts to “cheat” have been reported to us since our public launch in 2016.

Third-Party Certification – Rationale

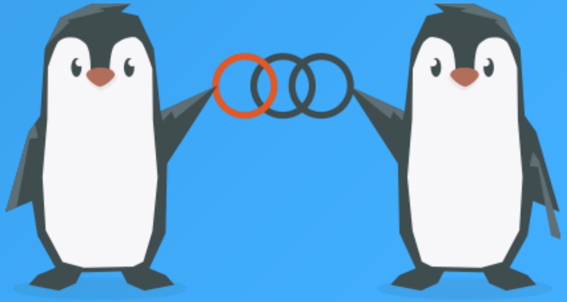
- Third-party certification to an OpenChain standard (and any other standard) one legal entity with appropriate permission in the local jurisdiction to certify that another legal entity meets the requirements of the relevant standard.

- This is a common approach in regulation-heavy industries such as automotive around standards such as ISO 26262 (functional safety).

- Because OpenChain produces ISO standards, it supports and follows the same type of third-party certification processes used by other ISO standards.

- Third-party certifiers such as Bureau Veritas and PwC support OpenChain standards.

Support Network



THE LINUX FOUNDATION

OPENCHAIN

We Have Community Study and Work Groups

Core Work Groups

Education (Autumn 2020~)

Specification (Spring 2016~)

Community Work Groups

Automation (Summer 2019~)

Community Study Groups

AI (January 2024~)

SBOM (July 2024~)

Industry-Specific Work Groups

Automotive (Summer 2019~)

Telecom (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~)

THE LINUX FOUNDATION

OPENCHAIN

We Have Free Reference Material

The OpenChain Project has extensive reference material:

- Reference open source training slides
- Policy template material
- Supplier education material
- Self-certification checklists and questionnaires
- + many, many more documents

We Have Commercial Support

Third-Party Certification

BUREAU VERITAS
CAICT 中国信通院
中国电子技术标准化研究院
CIC 工信安全
Deloitte.
ISCAS
KOSYAS
ORCRO
OSPOCO
pwc
SYNOPSYS
TIMETOACT SOFTWARE & CONSULTING
TÜV NORD
TÜV SÜD

Tooling / Automation

CIC 工信安全
C/Ɔ CYBELLUM
FOSSA
FOSSID
MEND
onward SECURITY
SCANOSS
SCANTIST
SECTREND
sonatype
棱镜七彩
SYNOPSYS
Trust Source
悬镜 XMIRROR

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
HH PARTNERS ATTORNEYS-AT-LAW
id est avocats
id law partners
JBB
理慈 Lee, Tsai & Partners
Lex Pan Law
LR29

Maggie Wang

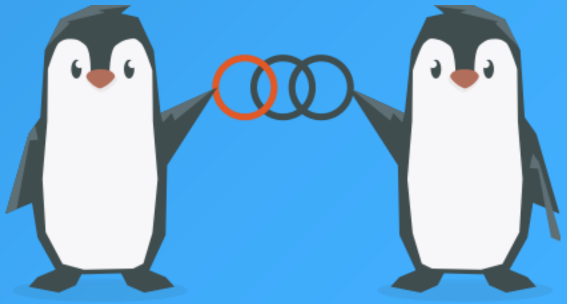
MCA
MOORCROFTS CORPORATE LAW
NORDEMANN
Osborne Clarke
StudioLegale.it
taylor | english
WITZEL ERB BACKU & PARTNER

Consultancies

{metæffekt}
AlektoMetis
bitsea.
CIC 工信安全
C/Ɔ CYBELLUM
Deloitte.
EACG Enterprise Architecture Consulting Group
FOSSAware
Hitachi Solutions
Lyra infosystems
NTT DATA Trusted Global Innovator
OSLN
Open Source Sense
Open TEKr
opsequ.io
ORCRO
OSADL
OSPOCO
OSS CONSULTANTS
pwc
SeQuenX
SOFTWARE COMPLIANCE ACADEMY
SOURCE Auditor
Source Code Control
SYNERGON
SYNOPSYS
TIMETOACT SOFTWARE & CONSULTING
TogánLabs
webpartner
wipro

THE LINUX FOUNDATION
OPENCHAIN

Relationship with Other Standards



THE LINUX FOUNDATION

OPENCHAIN

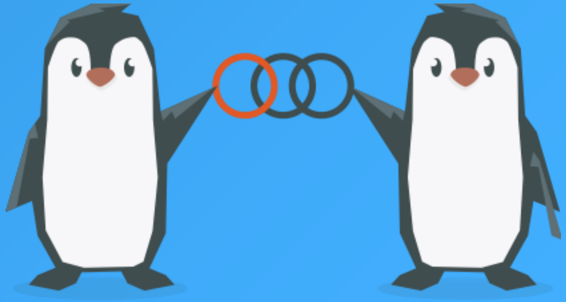
Wide Compatibility

- OpenChain standards are compatible with all compliance standards, security standards and SBOM formats that we are aware of.

- In general, OpenChain standards are designed to work with all other standards related to open source process management or solution implementation.

- The goal is to be practical and useful for companies of all sizes and in all markets.

Supporting Regulation



Addressing the CRA

- OpenChain ISO/IEC 5230 and ISO/IEC 18974 asked for record-keeping before Cyber Resiliency Act (CRA) made it into a requirement.

- OpenChain ISO/IEC 5230 and ISO/IEC 18974 require companies to create and archive verification materials around open source license compliance and security assurance.

Example Reference Material

THE LINUX FOUNDATION

OPENCHAIN

Recent Releases

Managing Your Open Source Software Supply Chain:

A Guide From The OpenChain Project

Second Edition

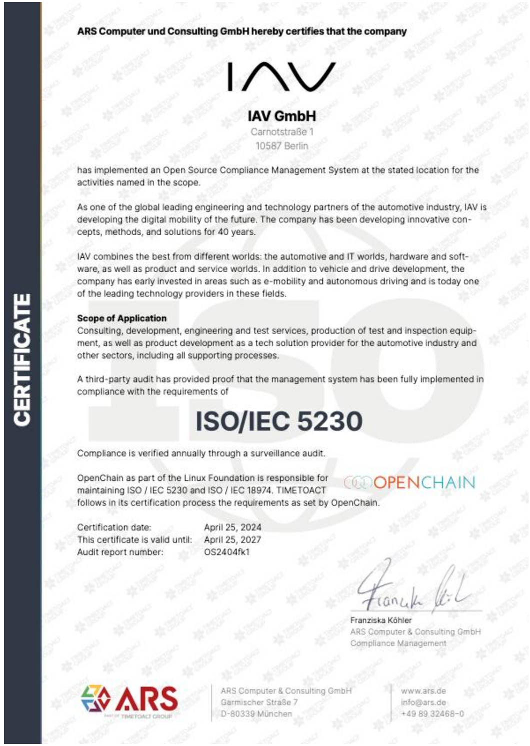
OpenChain Telco SBOM Guide:

A Guide From The OpenChain Project

THE LINUX FOUNDATION

OPENCHAIN

Case Studies



CERTIFICATE

ARS Computer und Consulting GmbH hereby certifies that the company

IAV

IAV GmbH
Carnotstraße 1
10587 Berlin

has implemented an Open Source Compliance Management System at the stated location for the activities named in the scope.

As one of the global leading engineering and technology partners of the automotive industry, IAV is developing the digital mobility of the future. The company has been developing innovative concepts, methods, and solutions for 40 years.

IAV combines the best from different worlds: the automotive and IT worlds, hardware and software, as well as product and service worlds. In addition to vehicle and drive development, the company has early invested in areas such as e-mobility and autonomous driving and is today one of the leading technology providers in these fields.

Scope of Application
Consulting, development, engineering and test services, production of test and inspection equipment, as well as product development as a tech solution provider for the automotive industry and other sectors, including all supporting processes.

A third-party audit has provided proof that the management system has been fully implemented in compliance with the requirements of

ISO/IEC 5230

Compliance is verified annually through a surveillance audit.

OpenChain as part of the Linux Foundation is responsible for maintaining ISO / IEC 5230 and ISO / IEC 18974. TIMETOACT follows in its certification process the requirements as set by OpenChain.

OPENCHAIN

Certification date:	April 25, 2024
This certificate is valid until:	April 25, 2027
Audit report number:	OS2404fk1

Franziska Köhler
ARS Computer & Consulting GmbH
Compliance Management

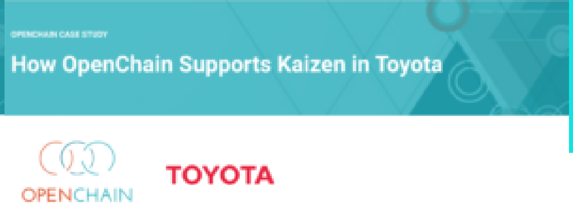
ARS
PART OF TIMETOACT GROUP

ARS Computer & Consulting GmbH
Garmischer Straße 7
D-80339 München

www.ars.de
info@ars.de
+49 89 32468-0

OPENCHAIN CASE STUDY

How OpenChain Supports the British NHS

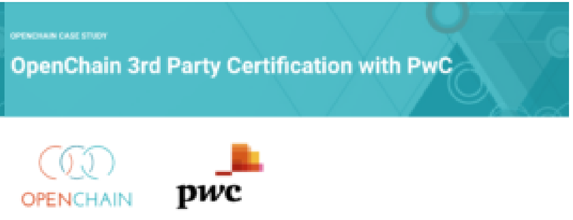


OPENCHAIN CASE STUDY

How OpenChain Supports Kaizen in Toyota

OPENCHAIN CASE STUDY

How OpenChain Supports Interneuron



OPENCHAIN CASE STUDY

OpenChain 3rd Party Certification with PwC

OPENCHAIN

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

BlackBerry, OSS Consultants and OpenChain

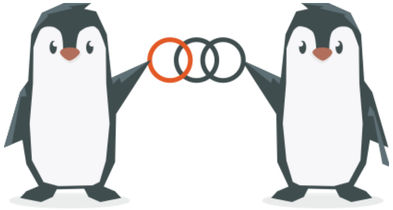
THE LINUX FOUNDATION

OPENCHAIN

Training Courses

Introduction to Open Source License Compliance Management (LFC193)

Implementing Open Source License Compliance Management (LFC194)



Data Point

90+

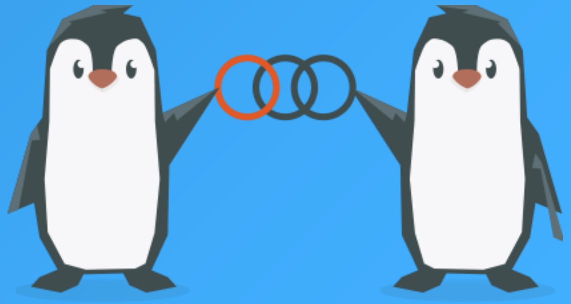
Webinars covering all aspects of open source management and governance

https://openchainproject.org/webinars

Always Evolving

THE LINUX FOUNDATION

OPENCHAIN



AI Work Group

Workshops and different timezone summary syncs are held once a month discussing AI Compliance in the supply chain. The study group is co-chaired by Matthew Crawford from Arm and David Marr from Qualcomm with a focus on identifying shared concerns across industries, and considering a guide about using AI BOM in the trusted supply chain.

April 2025

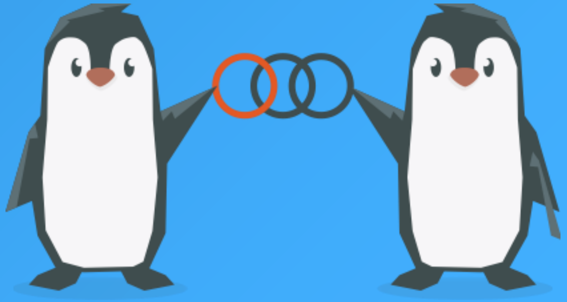
SBOM Study Group

The OpenChain Project has required Software Bill of Materials for its standards since 2016. Over the years, we have contributed to the field by developing SPDX Lite (a simple SBOM for suppliers) and releasing a guide to define SBOM Quality. In July we launched a new monthly Study Group to bring all our various activities together and answer the question of "how do we use SBOMs in production?" Regular meetings started in September.

March 2025

THE LINUX FOUNDATION OPENCHAIN

In Conclusion



THE LINUX FOUNDATION

OPENCHAIN

What Is Coming Next For The Market?

There is a steady, inevitable trend:

- Open source is becoming more professional
- Open source is becoming more accountable
- Open source is becoming more sustainable

In 2025 the OpenChain Project expects this trend to bring open source closer to traditional Software Asset Management (SAM).

What Will The OpenChain Project Do?

1. We will continue to assist in the professionalization of the supply chain, with specific impact in procurement, M&A and supply chain management

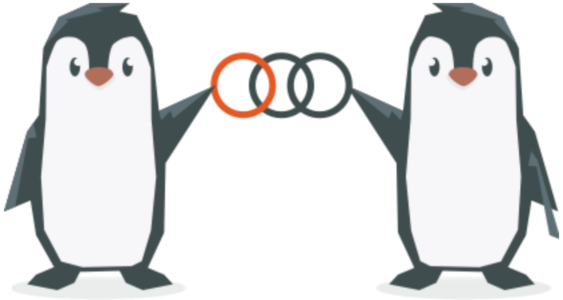
2. We will continue to grow our reference library of material to assist companies adopting and using our standards.

3. We will also support process management discussions in new domains like AI Compliance

Track All This Work

- Our calls are open and publicly listed.
- We publish a recording of every meeting not under Chatham House Rule.
- We provide access to work groups, special interest groups and local work groups via mailing list.
- We also use Slack and WeChat.

Let’s Talk More



Shane Coughlan
scoughlan@linuxfoundation.org
+81 80 4035 8083