

# Understanding How Open Source Is Managed Professionally in 2024

The View from Supply Chain Process Management

---

Shane Coughlan  
OpenChain Project



# CONTENTS

- 01 Moving from Unknown to Known
- 02 Progress of Evolution
- 03 Usage Methods
- 04 Support Material and Network
- 05 Market Developments
- 06 Conclusion





01

**Moving from Unknown to Known**

# Stacking Standards + Solutions

Process Management Standards

OPENCHAIN

Implementation Standards

SPDX

Methods

CHAOSS

TODO

# 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*

# Get Full Overviews Online

ISO/IEC 5230:2020  
Open Source License Compliance

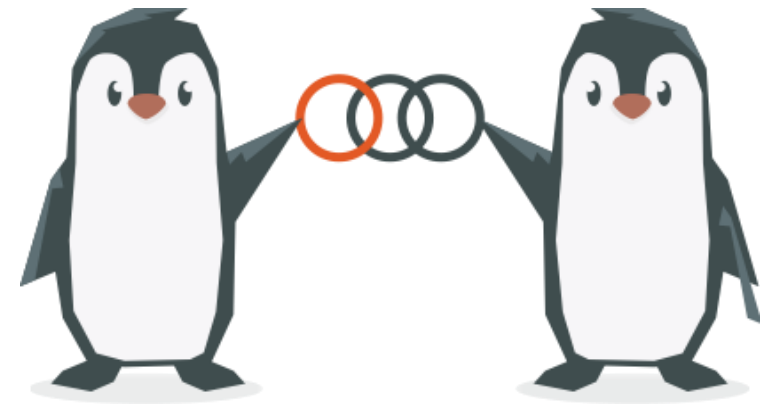


ISO/IEC 18974:2023  
Open Source Security Assurance



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.**







02

## Progress of Evolution

# A Continual Heartbeat Of Adoption

OpenChain standards are built, used  
and supported by all industries

Recent adoption announcements:



# Nokia Adoption of ISO/IEC 5230

NOKIA



# OpenHarmony Adoption of ISO/IEC 5230



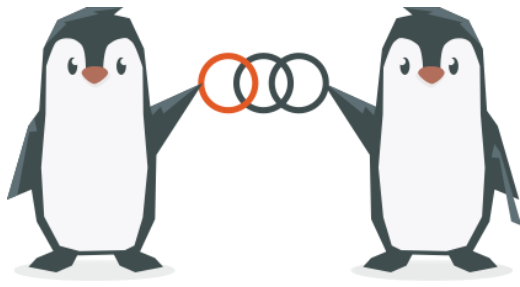
# Korea Telecom Adoption of ISO/IEC 18974



# Samsung SDS Adoption of ISO/IEC 18974

## **SAMSUNG SDS**

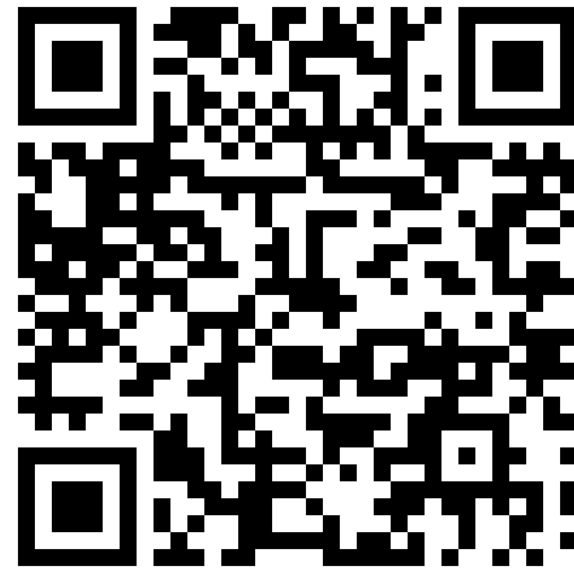




Data Point

31%

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





03

# Usage 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)
  - And OpenChain standards 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 extraordinarily 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.



04

# Support Material and Network

# OpenChain 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~)

## **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~)



# Existing 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



# 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



# Case Studies

CERTIFICATE

ARS Computer und Consulting GmbH hereby certifies that the company



**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.

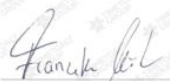
A third-party audit has provided proof that the management system has been fully implemented in compliance with the requirements of

**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.

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 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



AB EHR Digital  
Electronic Health Records

Source Code Control

OPENCHAIN CASE STUDY

## How OpenChain Supports Kaizen in Toyota



TOYOTA

OPENCHAIN CASE STUDY

## How OpenChain Supports Interneuron



Interneuron

OPENCHAIN CASE STUDY

## OpenChain 3rd Party Certification with PwC



### 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



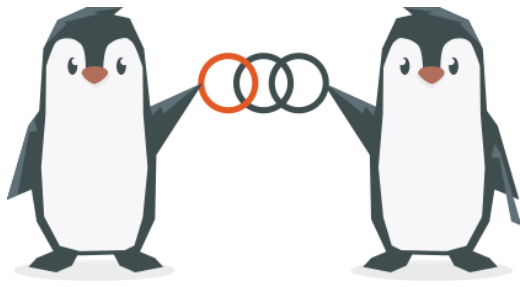


# Training Courses

**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>

# Webinars: AI Legal Landscape + Data Supply Chain

AI - The Current Legal Landscape

OpenChain Webinar





**GTC**

LAWYERS + STRATEGISTS



Anthony Decicco



Shea Leitch



Stanislav Zakharenko





Wael Nackasha




The Role of Data in the Supply Chain of AI

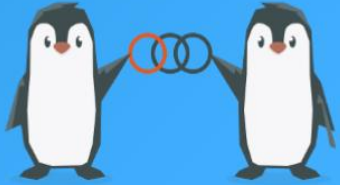
OpenChain Webinar







Nick Schifano



# October: CC-0 Maturity Model

## OpenChain Education Work Group

Sync Call for Asia: Deep Dive into Maturity Models



# Commercial Support

## Third-Party Certification



## Tooling / Automation



## Legal Providers



## Consultancies





05

# Market Developments

# Emerging Trends in Procurement Negotiations

ISO/IEC 5230 and ISO/IEC 18974 are a simple “ask” for procurement in all industries.

In the 2025 period we expect:

- More use of industry standards versus custom approaches for procurement
- More use of OpenChain standards

# Emerging Trends in Mergers and Acquisitions

ISO/IEC 5230 and ISO/IEC 18974 are a “floor” to check risk management in M&A.

In the 2025 period we expect:

- More use of OpenChain standards for M&A
- More case studies around the use of OpenChain standards



# Emerging Trends in Supply Chain Management

ISO/IEC 5230 and ISO/IEC 18974 make it easy for customers to check open source license compliance and security assurance.

In the 2025 period we expect:

- More supply chain requests for OpenChain use
- Open source maturity models describing OpenChain standards

# Addressing US Executive Order / NIST / CISA

- OpenChain ISO/IEC 5230 and ISO/IEC 18974 require the use of SBOMs.
- They are flexible enough to meet any specific requirements the US develops around SBOM use, structure or format.

# 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.

# 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.

# Policy Briefing Series:

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



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





06

**Conclusion**

# What Is Happening Right Now?

- An increase in the use of all types of formal standards around open source management
- An increase in the use of OpenChain standards for licensing and security
- Improved trust in the supply chain because of this

In 2025 the OpenChain Project expects awareness and capability around open source standards to become critical for companies.

# 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?

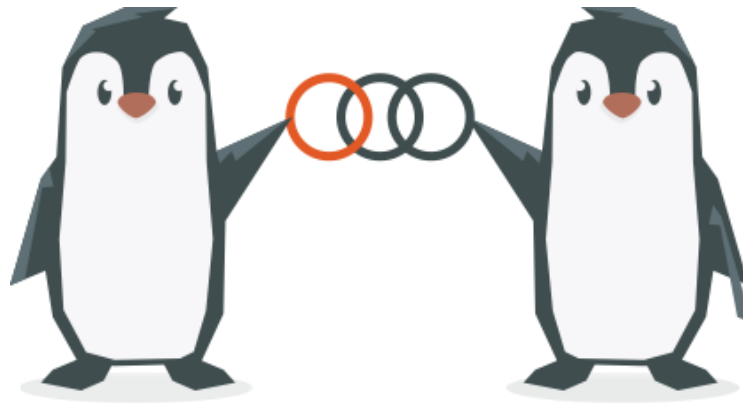
1. We will continue to assist in the professionalization of the supply chain, with specific impact in procurement, M&A and supply chain management
2. We will continue to grow our reference library of material to assist companies adopting and using our standards.
3. We will also support process management discussions in new domains like AI Compliance

# Track All This Work

- Our calls are open and publicly listed.
- We publish a recording of meetings 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

